

Федеральное государственное бюджетное образовательное учреждение
высшего образования «Московский государственный технический университет
им. Н.Э. Баумана (национальный исследовательский университет)»
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Калужский филиал МГТУ имени Н.Э. Баумана
(национальный исследовательский университет)»

НАУКОЕМКИЕ ТЕХНОЛОГИИ В ПРИБОРО- И МАШИНОСТРОЕНИИ И РАЗВИТИЕ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В ВУЗЕ

**Материалы
Всероссийской научно-технической конференции**

Том 2



Калуга 2020

УДК 378:001.891
ББК 74.58:72
Н34

Руководитель конференции:

А.В. Царьков (директор КФ МГТУ им. Н.Э. Баумана),
А.А. Столяров (зам. директора по научной работе)

Оргкомитет конференции:

Председатель оргкомитета: *Столяров А.А.*
Ученый секретарь: *Лебедев В.В.*

Члены оргкомитета:

<i>Андреев В.В.</i> д.т.н., профессор	<i>Корнюшин Ю.П.</i> д.т.н., профессор
<i>Косушкин В.Г.</i> д.т.н., профессор	<i>Ильин В.В.</i> д.филос.н., профессор
<i>Коржавый А.П.</i> д.т.н., профессор	<i>Горбунов А.К.</i> д.ф-м.н., профессор
<i>Шаталов В.К.</i> д.т.н., профессор	<i>Перерва О.Л.</i> д.э.н., профессор
<i>Мазин А.В.</i> д.т.н., доцент	<i>Рамазанов А.К.</i> к.ф-м.н., доцент
<i>Мальшев Е.Н.</i> к.т.н., доцент	<i>Мельников Д.В.</i> к.т.н., доцент
<i>Пономарев А.И.</i> к.т.н., доцент	<i>Анкудинов А.А.</i> к.т.н., доцент
<i>Шубин А.А.</i> к.т.н., доцент	<i>Максимов А.В.</i> к.т.н., доцент
<i>Сломинская Е.Н.</i> к.т.н., доцент	<i>Орлик Г.В.</i> к.т.н., доцент
<i>Пащенко В.Н.</i> к.т.н., доцент	<i>Жинов А.А.</i> к.т.н., доцент

Н34 **Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе:** материалы Всероссийской научно-технической конференции, 17–19 ноября 2020 г. Т. 2. – Калуга: Издательство МГТУ им. Н. Э. Баумана, 2020. –250 с.

В сборнике материалов Всероссийской научно-технической конференции представлены результаты научных исследований, выполненных учеными в течение ряда лет. Систематизированы материалы различных научных школ. Результатами научных исследований являются новые методы, вносящие вклад в развитие теории, а также прикладные задачи, воплощенные в конструкции и материалы.

УДК 378:001.891
ББК 74.58:72

© Коллектив авторов, 2020
© Калужский филиал МГТУ
им. Н. Э. Баумана, 2020
© Издательство МГТУ
им. Н. Э. Баумана, 2020

СЕКЦИЯ 8.

ЗАЩИТА ИНФОРМАЦИИ

АЛГОРИТМ СОЗДАНИЯ QR-КОДА

QR код – это монохромная картинка, на которой некоторые устройства (например смартфон со специальным приложением) распознают текст.

Сегодня, когда QR-коды достаточно распространены, их создание занимает очень мало времени и не требует каких-либо специальных знаний. Чтобы создать QR-код, необходимо зайти на один из множества сайтов, позволяющих создавать такие коды, ввести информацию, которую вы хотите зашифровать, и сайт выдаст готовый графический QR-код.

Сайт не позволяет пользователю увидеть, что происходит с информацией и как она становится QR-кодом, но алгоритм шифрования давно известен. QR-код формируется по строго определенному алгоритму, который в упрощенном виде можно разделить на несколько этапов [1]:

- Кодирование данных.
- Добавление служебной информации.
- Разделение информации на блоки.
- Создание байтов коррекции.
- Объединение блоков.
- Размещение информации на QR коде.

Кодирование данных. QR код поддерживает несколько способов кодирования данных, в зависимости от того, какие символы используются: цифровое, буквенно-цифровое, кандзи (китайско-японские иероглифы) и побайтовое кодирование.

Максимальное число символов, которое можно внести в QR-код:

- Цифры – 7089;
- Цифры и буквы латинского алфавита – 4296;
- Иероглифы – 1817;
- Двоичный код – 2953 байта (около 2953 букв кириллицы в кодировке windows-1251 или 1450 букв кириллицы в utf-8).

Цифровое кодирование требует 10 бит на 3 символа. Вся последовательность символов разбивается на группы по 3 цифры, и каждая группа (трёхзначное число) переводится в 10-битное двоичное число и добавляется к последовательности бит.

При буквенно-цифровом кодировании на 2 символа требуется 11 бит информации. Входной поток символов разделяется на группы по 2, в группе каждый символ кодируется согласно таблице внизу, значение первого символа в группе умножается на 45 и прибавляется к значению второго символа. Полученное число переводится в 11-битное двоичное число и добавляется к последовательности бит.

Побайтовое кодирование – это универсальный способ кодирования, которым можно закодировать любые символы. Единственным недостатком

метода является относительно низкая плотность информации. В этом случае текст кодируется в любой кодировке (рекомендуемо в UTF-8) и полученная последовательность байт берётся в неизменном виде.

Добавление служебной информации. На данной стадии формирования QR-кода определяется уровень коррекции ошибок и версия кода, а также происходит добавление служебных полей, в которых указывается способ кодирования и количество данных.

Всего QR-коды имеют 4 уровня коррекции ошибок, которые отличаются количеством информации для восстановления и, соответственно, количеством полезной информации, которую можно восстановить при повреждении кода:

- L–уровень коррекции. При его использовании можно восстановить 7 % информации;
- M–уровень коррекции. Восстановление 15 % информации;
- Q–уровень коррекции. Восстановление 25 % информации.
- H–уровень коррекции. Восстановление 30 % информации.

Для исправления ошибок используется алгоритм Рида-Соломона. Данный алгоритм используется как при создании QR-кода, так и при его дешифрации.

Ещё одно свойство QR кода – его версия (чем она больше, тем больше размер). Всего существует 40 версий. Номер версии зависит от количества кодируемой информации и от уровня коррекции.

Служебные поля записываются перед последовательностью бит, полученной в предыдущем пункте.

Способ кодирования – поле длиной 4 бита, которое имеет следующие значения: 0001 для цифрового кодирования, 0010 для буквенно-цифрового и 0100 для побайтового.

Количество данных – это количество кодируемых символов, а для побайтового – количество байт в полученной последовательности, представленное в виде двоичного числа определённой длины.

Разделение информации на блоки. Последовательность байт, полученная на предыдущем этапе, разделяется на определённое для версии и уровня коррекции количество блоков.

Процесс основан на алгоритме Рида-Соломона. Он должен быть применён к каждому блоку информации QR-кода. Сначала определяется количество байт коррекции, которые необходимо создать, а затем, с ориентиром на эти данные, создаётся многочлен генерации. Количество байтов коррекции на один блок определяются по выбранной версии кода и уровню коррекции ошибок. По количеству байтов коррекции определяется генерирующий многочлен.

Расчёт производится исходя из значений исходного массива данных и значений генерирующего многочлена, причём для каждого шага цикла отдельно.

Объединение блоков. Из каждого блока данных по очереди берётся один байт информации, когда очередь доходит до последнего блока, из него берётся байт и очередь переходит к первому блоку. Так продолжается до тех пор, пока

в каждом блоке не кончатся байты. Аналогичным образом надо сделать с блоками байтов коррекции. Они берутся в том же порядке, что и соответствующие блоки данных.

Размещение информации на QR коде. На QR-коде есть обязательные поля, они не несут закодированной информации, а содержат информацию для декодирования (рис. 1) [3]:

- Поисковые узоры – это 3 квадрата по углам кроме правого нижнего. Используются для определения расположения кода. Эти объекты имеют размер 8x8 модулей.
- Выравнивающие узоры – появляются, начиная со второй версии, используются для дополнительной стабилизации кода, более точном его размещении при декодировании. Итоговый размер выравнивающего узора – 5x5. Стоят такие узоры на разных позициях в зависимости от номера версии.
- Полосы синхронизации – используются для определения размера модулей. Располагаются они уголком, начинается одна от левого нижнего поискового узора, идёт до левого верхнего, а оттуда начинается вторая, по тому же правилу, заканчивается она у правого верхнего. Выглядят полосы синхронизации как линии чередующихся между собой чёрных и белых модулей.
- Код маски и уровня коррекции – расположен рядом с поисковыми узорами: под правым верхним и справа от левого нижнего, и дублируются по бокам левого верхнего.
- Код версии (с 7-й версии) – находятся слева от верхнего правого и сверху от нижнего левого, причём дублируются.

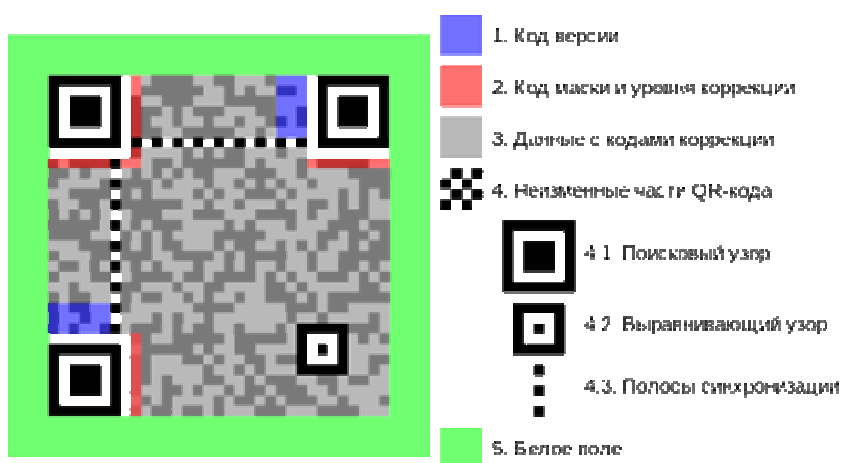


Рис. 1. Описание полей QR-кода

Оставшееся свободным место делят на столбики шириной в 2 модуля и заносят туда информацию, причём делают это «змейкой». Заполнение начинается с правого нижнего угла, идёт в пределах столбика справа налево, снизу вверх. Если достигнут верх столбика, то движение продолжается с верхнего правого угла столбика, который расположен левее, и идёт сверху

вниз. Достигнув низа, движение продолжается от нижнего правого угла столбика, который расположен левее, и идёт снизу вверх. И так далее, пока всё свободное пространство не будет заполнено (рис. 2).

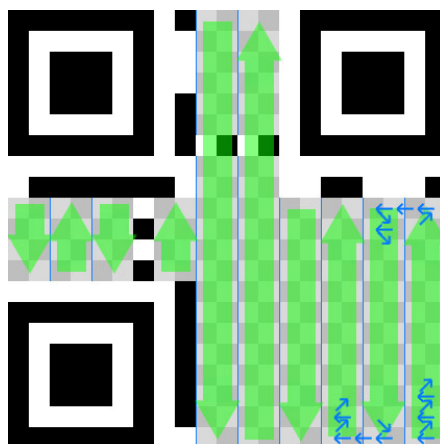


Рис. 2. Порядок заполнения QR-кода данными

Алгоритм создания QR-кода может показаться не таким сложным, но на сегодняшний день в интернет-пространстве есть достаточно широкий выбор онлайн сервисов для генерирования QR-кодов, поэтому, если вы не собираетесь создавать собственный автоматический генератор, будет надежнее воспользоваться проверенными сервисами. В качестве примера можно привести онлайн ресурс <http://qrcoder.ru/> или офлайн программу QR CodeStudio [2].

Список литературы

- [1]. Ковалёв А.И. QR-коды, их свойства и применение / А.И. Ковалёв. – Текст : непосредственный // Молодой ученый. – 2016. – № 10 (114). – С. 56-59.
- [2]. Ковальчук Василь. Технология QR-кодировки: инновационный метод предоставления информации. – 2019. – С. 253–256.
- [3]. *Wikipedia*: свободная энциклопедия [Электронный ресурс]. – <https://ru.wikipedia.org>. – [дата обращения: 05.11.2020].

Войцев Константин Юрьевич – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: voishchevkostya@gmail.com

АНАЛИЗ ЗАЩИЩЕННОСТИ И УЯЗВИМОСТЕЙ ИГРОВЫХ ДВИЖКОВ

Игровой движок – центральный программный компонент любой игры или другого интерактивного приложения, использующего графические вычисления. Он обеспечивает основные технологии, средства и инструменты, необходимые для создания игры, а затем объединяет их воедино. Движок затрагивает все компоненты игры, такие как рендеринг, физические расчеты, звуковое оформление, создание искусственного интеллекта, скриптинг и сетевые взаимодействия. Благодаря средствам движка у разработчиков есть возможность выпускать свои игры сразу на нескольких платформах, таких как персональные компьютеры, мобильные устройства и игровые консоли, с минимальными затратами ресурсов на портирование.

Игровые движки, как и другие программные продукты, могут быть подвержены атакам на информационную безопасность. Наиболее вероятной угрозой является несанкционированный доступ к исходным данным продукта, созданного на основе игрового движка (программный код, ресурсы, ассеты). Также, воспользовавшись одной из уязвимостей, злоумышленники могут намеренно нарушить целостность игры вызвать неправильную работу. Далее проводится анализ защищенности некоторых игровых движков.

Unity. Unity – бесплатное для коммерческого использования программное обеспечение, предназначенное для кроссплатформенной разработки компьютерных игр. Unity позволяет создавать приложения для более чем 25 различных платформ. Платформой разработки на Unity является .NET Framework.

Unity поддерживает 2 метода компиляции проектов – Mono и IL2CPP (Intermediate Language To C++).

Mono – платформа, воплощающая в себя .NET Framework на базе свободного программного обеспечения. Включает в себя компилятор языка C#, среду исполнения .NET (с поддержкой Just-in-time-компиляции «на лету»), отладчик, а также ряд библиотек.

В процессе сборки вся логика, написанная на языке C#, компилируется в код на языке Common Intermediate Language (CIL), который управляется средой Common Language Runtime (CLR). Далее, непосредственно во время выполнения программы, она преобразует исполняемые в данный момент участки IL-кода в машинный код. Это и есть JIT-компиляция. Схема процесса компиляции приложения, собранного с помощью Mono, представлена на рис. 1.

IL2CPP – более современная, по сравнению с Mono, платформа, созданная непосредственно Unity Technologies. Технология IL2CPP состоит из 2 частей: Ahead-of-time компилятора (AOT-компиляция перед исполнением) и исполняемой библиотеки для поддержки виртуальной машины.

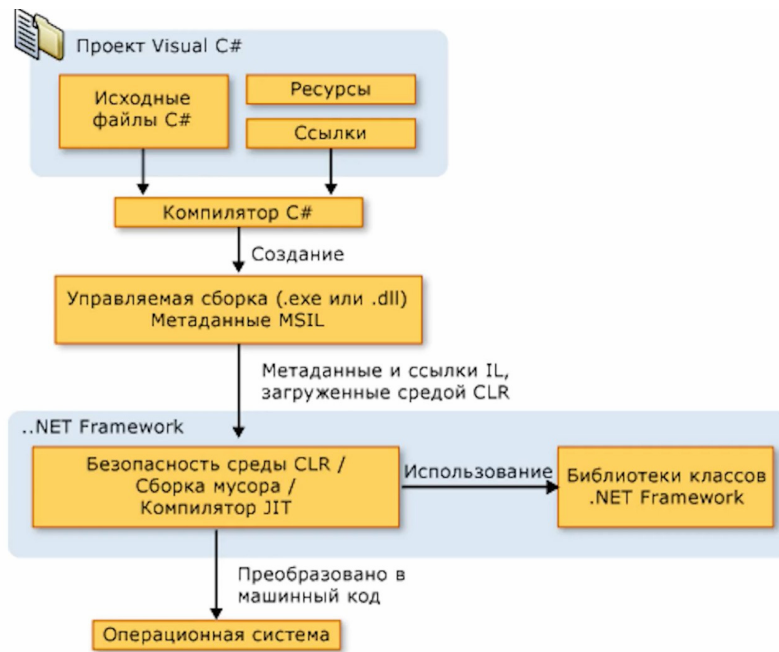


Рис. 1. Схема процесса компиляции приложения, собранного с помощью Mono

Отличием от Mono является то, что после того, как был создан управляемый IL-код, AOT-часть сборки не считается завершенной. Внутренний компилятор Unity анализирует IL-код на предмет неиспользуемых частей кода и удаляет их. Затем урезанные сборки с помощью AOT-компилятора IL2CPP.exe конвертируются в код на языке C++, который преобразуется непосредственно в машинный код. Схема процесса компиляции приложения, собранного на IL2CPP представлена на рис. 2 [1].

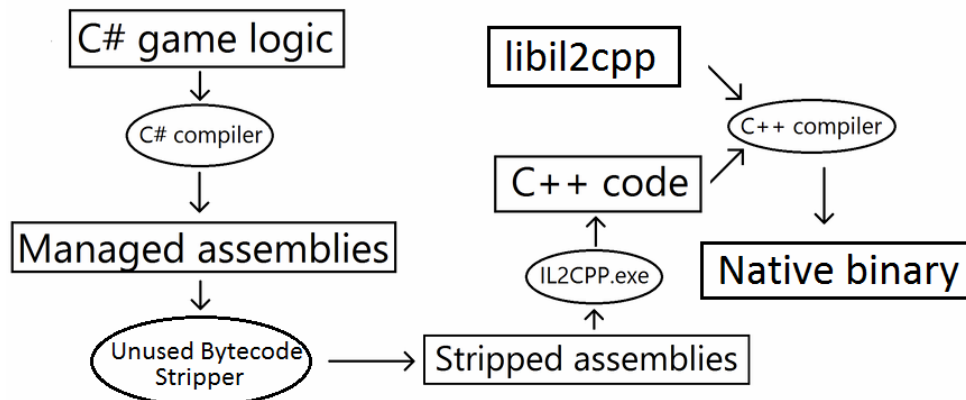


Рис. 2. Схема процесса компиляции приложения, собранного на IL2CPP

Плюсом IL2CPP, по сравнению с Mono, является увеличение уровня безопасности сборки, поскольку проект, собранный на Mono, хранит в себе dll-файлы (Dynamic Link Library), которые с помощью определенных декомпиляторов CIL (ILSpy, DnSpy – это открытые бесплатные) легко конвертируются обратно в проект на языке C#, в то время как IL2CPP-сборка не имеет такого недостатка: вся логика хранится в исполняемом файле. Его полноценная декомпиляция нереальна, все имена функций и переменных будут поте-

ряны, также велика вероятность возникновения различных ошибок при попытке запустить проект. Возможно лишь дизассемблирование исполняемого файла, что существенно усложняет чтение и изменение. Такой подход не позволяет украсть чужой исходный код и переиспользовать его где-либо еще. Также уменьшается общий размер проекта [2].

Минусом IL2CPP является лишь более долгое время сборки проекта по сравнению с Mono.

Ресурсы игры (текстуры, 3d-модели, шрифты, анимации, звуки и т. д.) в Unity нельзя считать безопасными, поскольку на момент написания статьи существуют программы (DEVx Unity Unpacker, Unity Assets Explorer), позволяющие получать к ним доступ и видоизменить.

Unreal Engine. Unreal Engine – игровой движок, разрабатываемый и поддерживаемый компанией Epic Games. Со 2 марта 2015 года является бесплатным, однако разработчики должны передавать 5% от выручки с продаж компании Epic Games, если ежеквартальная выручка превышает 3000\$. Данный движок написан на языке C++ и позволяет создавать игры для большого числа операционных систем и платформ, как мобильных, так и стационарных (Microsoft Windows, Linux, Mac OS и Mac OS X; консолей Xbox, Xbox 360, Xbox One, PlayStation 2, PlayStation 3, PlayStation 4, PSP, PS Vita, Wii, Dreamcast, GameCube). Игровая логика создается средствами языка C++ либо с помощьюBlueprintов (Blueprints) – системы визуального скриптинга, созданной компанией Epic Games.

Для упрощения портирования движок использует модульную систему зависимых компонентов; поддерживает различные системы рендеринга (Direct3D, OpenGL, Pixomatic; в ранних версиях: Glide, S3, PowerVR), воспроизведения звука (EAX, OpenAL, DirectSound3D; ранее: A3D), средства голосового воспроизведения текста, распознавание речи, модули для работы с сетью и поддержки различных устройств ввода.

Как было указано выше, игры на Unreal Engine разрабатываются на языке C++, следственно для сборки проекта используется компилятор этого языка (MSVC для сборки под Windows и Clang для сборки под платформы Unix-семейства). На выходе получается исполняемый файл, хранящий в себе всю логику. Полноценно декомпилировать его, получив изначальный исходный код невозможно, а процесс чтения ассемблерного кода достаточно трудоемок, для еще большего его усложнения можно использовать обфускаторы. Следственно украсть и переиспользовать код проекта, созданного средствами Unreal Engine практически невозможно, а попытка его изменения, скорее всего, приведет к неработоспособности игры, а не к получению каких-либо выгод.

Также Unreal Engine имеет функцию шифрования ресурсов игры с помощью алгоритма AES 256. Это означает, что получить доступ к уже запакетованным ресурсам игры можно только с помощью 256-битного ключа, который генерируется в процессе сборки. На данный момент, ссылаясь на некоторые источники можно сказать, что при лучших исходах для взлома такого алгоритма и подбора ключа понадобится 31 557 600 лет. Из этого факта мож-

но сделать вывод, что злоумышленник не сможет получить доступ к зашифрованным ресурсам, а следственно их кража и переиспользование практически невозможны [3].

Source 2. Source 2 – игровой движок, разработанный американской компанией Valve Corporation. В отличие от первой версии, которая была создана исключительно для использования внутри компании, доступен бесплатно с той лишь оговоркой, что продукты, созданные на Source 2, должны быть распространяться эксклюзивно на платформе Steam (Steam – онлайн-сервис цифрового распространения компьютерных игр и программ, разработанный и поддерживаемый Valve Corporation). Данный движок был анонсирован 3 марта 2015 года, а 21 ноября 2019 года был представлен Valve Hammer Editor – набор инструментов, поддерживающий работу с Source 2. Движок написан на языке C++ и позволяет разрабатывать игры практически для любых платформ самим Valve, но пользователи, ограниченные соглашением, могут создавать свои продукты лишь для Windows, Linux и MacOS.

Игры, созданные с помощью Source, пишутся на языке C++. В комплекте с библиотеками самого движка идет исходный код игры Half Life 2 и всех ее эпизодов, также написанный на C++. Исходя из выводов, сделанных в предыдущих частях статьи о защите кода, написанного на C++, можно сказать, что исходный код игр, разработанные на Source 2 хорошо защищены, чего нельзя сказать о ресурсах: они представляют собой Valve Pak (VPK)-файл, который является несжатым архивом, хранящим себе весь или некоторую часть игрового контента. Такой архив может быть распакован, просмотрен, изменен и запакован обратно с помощью таких программ как Valve Resources Viewer, GCFSScape, следственно формат хранения ресурсов движка Source нельзя считать безопасным [4].

Память игры. Во всех рассмотренных игровых движках значения переменных хранятся в своём изначальном виде, без какой-либо защиты. Злоумышленнику не составит проблем с помощью стороннего программного обеспечения найти нужные ему данные в оперативной памяти и изменить их. Примером такого программного обеспечения является Cheat Engine.

Cheat Engine – это бесплатный сканер/отладчик памяти с открытым исходным кодом для операционной системы Windows. Он выполняет поиск значений, вводимых пользователем, с помощью широкого спектра опций, которые позволяют пользователю находить и сортировать данные в памяти компьютера.

Вывод. На основе проведенного анализа можно сделать вывод, что Unreal Engine является наиболее безопасным из рассмотренных движков, поскольку в нем защищены как исходный код разрабатываемой игры, так и ресурсы. Самым уязвимым же является Unity, а именно частный случай сборки проекта с помощью Mono, так как в случае взлома такой сборки злоумышленник может получить доступ не только к ресурсам игры, но и к исходному коду.

Список литературы

- [1]. *Lavieri E.* Getting Started with Unity 2018 // Third Edition, Packt Publishing Ltd., 2018
- [2]. *Zucconi A.* A practical tutorial to hack (and protect) Unity games, 2015
URL: <http://www.alanzucconi.com/2015/09/02/a-practical-tutorial-to-hack-and-protect-unity-games/> (дата обращения 30.10.2020)
- [3]. *Edmonds M.* Mastering Game Development with Unreal Engine 4 // Second Edition By Matt Edmonds, Packt Publishing Ltd., 2018
- [4]. *Bernier B.* Source SDK Game Development Essentials // Packt Publishing Ltd., 2014

Бабкин Артём Андреевич – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: dr.v991149@gmail.com

Глебов Игорь Владимирович – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: igor.glebov1999@mail.ru

Лачихина Анастасия Борисовна – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anastasialach73@gmail.com

АНАЛИЗ ЗАЩИЩЁННОСТИ ИНФОРМАЦИИ, ЗАКОДИРОВАННОЙ В QR-КОДЕ, И МЕХАНИЗМОВ ЗАСЕКРЕЧИВАНИЯ ИНФОРМАЦИИ

Безопасность информации, закодированной в QR-коде, становится довольно обсуждаемой проблемой во всём мире. Тем не менее, важно отметить, что технология QR-кода сама по себе не имеет проблем с безопасностью. QR-коды не могут быть взломаны. Статические QR-коды являются машиночитаемыми, и содержимое внутри них не может быть изменено после генерации. Содержимое внутри динамического QR-кода, однако, может быть изменено, но для этого необходимо получить доступ к учётной записи пользователя, который создал их. Риски безопасности информации возникают в случае, если злоумышленники встраивают вредоносное программное обеспечение или веб-сайты в информацию, закодированную в QR-коде [1].

Потенциальная проблема безопасности информации, закодированной в QR-коде. Как показал опыт внедрения QR-кодов в Китае, технологию с успехом освоили не только пользователи, но и злоумышленники. С её помощью киберпреступники успешно крадут денежные средства и конфиденциальную информацию. Проблема заключается в том, что отличить легитимный QR-код от QR-кода злоумышленника визуально невозможно. Если торговая точка использует статический QR-код, киберпреступник может просто заклеить его своим. Подменить код генерации динамического QR-кода в автоматизированной точке тоже не так трудно.

В связи с этим появились два распространённых угроз безопасности информации, связанных с QR-кодами, но не с самой технологией.

Фишинг QR-кода. Объявления для веб-сайтов часто содержат QR-коды, которые направляют пользователей на определённую целевую страницу. Злоумышленник, подменяя QR-код, перенаправляет пользователя на вредоносный сайт. Цифровая среда не единственное место, где возможен фишинг QR-кода. Хакеры также могут размещать печатные QR-коды в общественных местах для сбора регистрационной информации пользователей. Это может быть особенно опасно, если эта информация предназначена для таких веб-сайтов, как интернет-банкинг или других, использующих конфиденциальные данные [2].

Вредоносное обеспечение. Данный риск безопасности, связан с загрузками, многие из которых направлены на пользователей мобильной операционной системы Android с открытым исходным кодом. Эта атака, известная как «Тайная загрузка», включает в себя направление пользователя на определённый веб-сайт, который автоматически начинает загрузку данных, без подтверждения пользователя. Использование QR-кодов значительно облегчает реализацию такой атаки, потому как ссылка вредоносного веб-сайта сокрыта в закодированной информации кода, а пользователи мобильных устройств

гораздо реже проверяют URL-адрес на корректность, чем пользователи персональных компьютеров.

Современный способ решения данной проблемы заключается в соблюдении следующих приёмов:

- проверки суммы перевода и наименования получателя перед подтверждением оплаты с помощью QR-кода;
- проверки того, что QR-код не наклеен поверх другого;
- проверка QR-кодов с помощью специальных приложений, распознающих вредоносный контент;
- генерация платёжного QR-кода на своём смартфоне непосредственно в момент оплаты для предотвращения перехвата злоумышленником в момент передачи;
- сокрытие генерации QR-кода для предотвращения визуального перехвата.

Одним из возможных способов решения данной проблемы может стать кодирование информации в QR-коде в зашифрованном виде. Информация, закодированная в подобный QR-код, может быть прочтена только доверенным приложением. Неосведомлённость злоумышленника о ключе шифрования не позволит изменить или встроить вредоносный код в такой QR-код. Таким образом, пользователь, используя мобильное приложение, может не только безопасно проводить операции с QR-кодами, но и подтверждать на основе их успешной расшифровки подлинность документа [3].

Список литературы

[1]. *What is a QR Code?* [Электронный ресурс]. – Режим доступа: [www.url: https://web.archive.org/web/20160605013533/http://www.qrcode.com/en//about/](https://web.archive.org/web/20160605013533/http://www.qrcode.com/en//about/). – (дата обращения: 22.10.2020)

[2]. *QR Code features* [Электронный ресурс]. – Режим доступа: [www.url: https://web.archive.org/web/20130129064920/http://www.qrcode.com/en/qrcodefeature.html](https://web.archive.org/web/20130129064920/http://www.qrcode.com/en/qrcodefeature.html). – (дата обращения: 22.10.2020)

[3]. *Somdip Dey, Asoke Nath.* (2019) Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System // arXiv.org URL: <https://arxiv.org/pdf/1808.05827.pdf> (дата обращения: 17.10.2020)

Курдюков Павел Русланович – студент БАС.И-91 КФ МГТУ им. Н.Э. Баумана, ООО «Кит-инвест». E-mail: Nyltarion@yandex.ru

Лачихина Анастасия Борисовна – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anastasialach73@gmail.com

В.В. Драган

АНАЛИЗ МЕТОДОВ ВЕРИФИКАЦИИ БЕЗОПАСНОСТИ ПО

Информационные технологии представляют собой совокупность вычислительных устройств, систем обработки информации, телекоммуникационных технологий и программного обеспечения. Они служат базой для экономической деятельности, социального и культурного развития человечества, обеспечивая людям доступ к информации.

Уровень безопасности информационных систем определяются многими факторами. Одним из важных факторов является безопасность программного обеспечения (ПО). Если не рассматривать ситуацию умышленного внедрения в код программных закладок, то проблема безопасности ПО связана с наличием в нем ошибок.

Основным методом повышения безопасности ПО является его верификация. Верификация проверяет соответствие между нормами стандартов, описанием требований (техническим заданием) к ПО, проектными решениями, исходным кодом, пользовательской документацией и функционированием самого ПО.

Обычно процесс верификации проводится сверху вниз, начиная от общих требований, заданных в техническом задании и/или спецификации на всю информационную систему, и заканчивая детальными требованиями к программным модулям и их взаимодействию.

Цели верификации ПО достигаются посредством последовательного выполнения комбинации из инспекций проектной документации и анализа их результатов, разработки тестовых планов тестирования и тест-требований, тестовых сценариев и процедур, и последующего выполнения этих процедур. Тестовые сценарии предназначены для проверки внутренней непротиворечивости и полноты реализации требований. Выполнение тестовых процедур должно обеспечивать демонстрацию соответствия испытываемых программ исходным требованиям.

Существует несколько методов верификации ПО. К основным относятся статический и динамический анализ, формальная верификация программ.

Статический анализ

Статический анализ кода – анализ программного обеспечения, производимый (в отличие от динамического анализа) без реального выполнения исследуемых программ.

Задачи, решаемые программами статического анализа кода, можно разделить на 3 категории:

1. Выявление ошибок в программах.

Рекомендации по оформлению кода. Некоторые статические анализаторы позволяют проверять, соответствует ли исходный код, принятому в компании стандарту оформления кода. Имеется в виду контроль количества отступов в

различных конструкциях, использование пробелов/символов табуляции и так далее.

2. Подсчет метрик. Метрика программного обеспечения – это мера, позволяющая получить численное значение некоторого свойства программного обеспечения или его спецификаций.

Проверенные на практике правила корректности кода или шаблоны типичных ошибок переносятся в среды разработки, такие как Eclipse или Microsoft Visual Studio, и постепенно становятся семантическими правилами языков программирования, их проверка возлагается на компиляторы этих языков. Поэтому статический анализ можно считать наиболее широко применяемым методом верификации.

При помощи системного анализа можно выявить следующие классы ошибок:

- а. неопределенное поведение программы;
- б. неинициализированные переменные;
- в. нарушение правил использования библиотекой;
- г. сценарии, приводящие к недокументированному поведению программы;
- д. переполнение буфера;
- е. ошибки в повторяющемся коде;
- ж. ошибки форматных строк.

Верификация методом статического анализа наиболее эффективна на этапе конструирования ПО, так как статический анализ применим к исходному тексту программы и не подразумевает её выполнения, это позволяет существенно снизить стоимость проекта и повысить его надежность. Инструменты автоматической верификации на основе статического анализа применяются достаточно широко, поскольку удобны и просты в использовании и не требуют специальной подготовки программы.

Динамический анализ

Это методы, в рамках которых анализ программного обеспечения осуществляется при помощи реального выполнения программы. На вход программы поступают последовательности данных, которые могут вызвать недетерминированное поведение, тем самым позволяя обнаружить уязвимости и ошибки.

Динамический анализ можно разделить на несколько видов:

1) Верификационный мониторинг

Верификационный мониторинг состоит в протоколировании функционирования программных продуктов в обычных режимах работы и оценки их соответствия требованиям и проектным решениям, а также выявления и регистрация ошибок, которые были допущены во время разработки или модификации программных продуктов.

Эффективность мониторинга программных продуктов может быть обеспечена только тогда, когда он осуществляется в рамках конкретных целей, то есть он должен затрагивать важные вопросы процесса разработки и создания программных продуктов. При мониторинге программных продуктов исполь-

зуются различные методы верификации. Эти методы различаются по своему назначению, видам регистрируемой информации, способу получения данных о работе программных продуктов, их анализа и т.д.

2) Тестирование

Тестирование программного обеспечения направлено на поиск тех ситуаций в программном коде, в которых поведение программы становится недетерминированным, не правильным и не соответствующим спецификации. Обычно тестирование осуществляется в рамках известных, заданных сценариев. На рис. 1 представлены основные виды тестирования ПО.

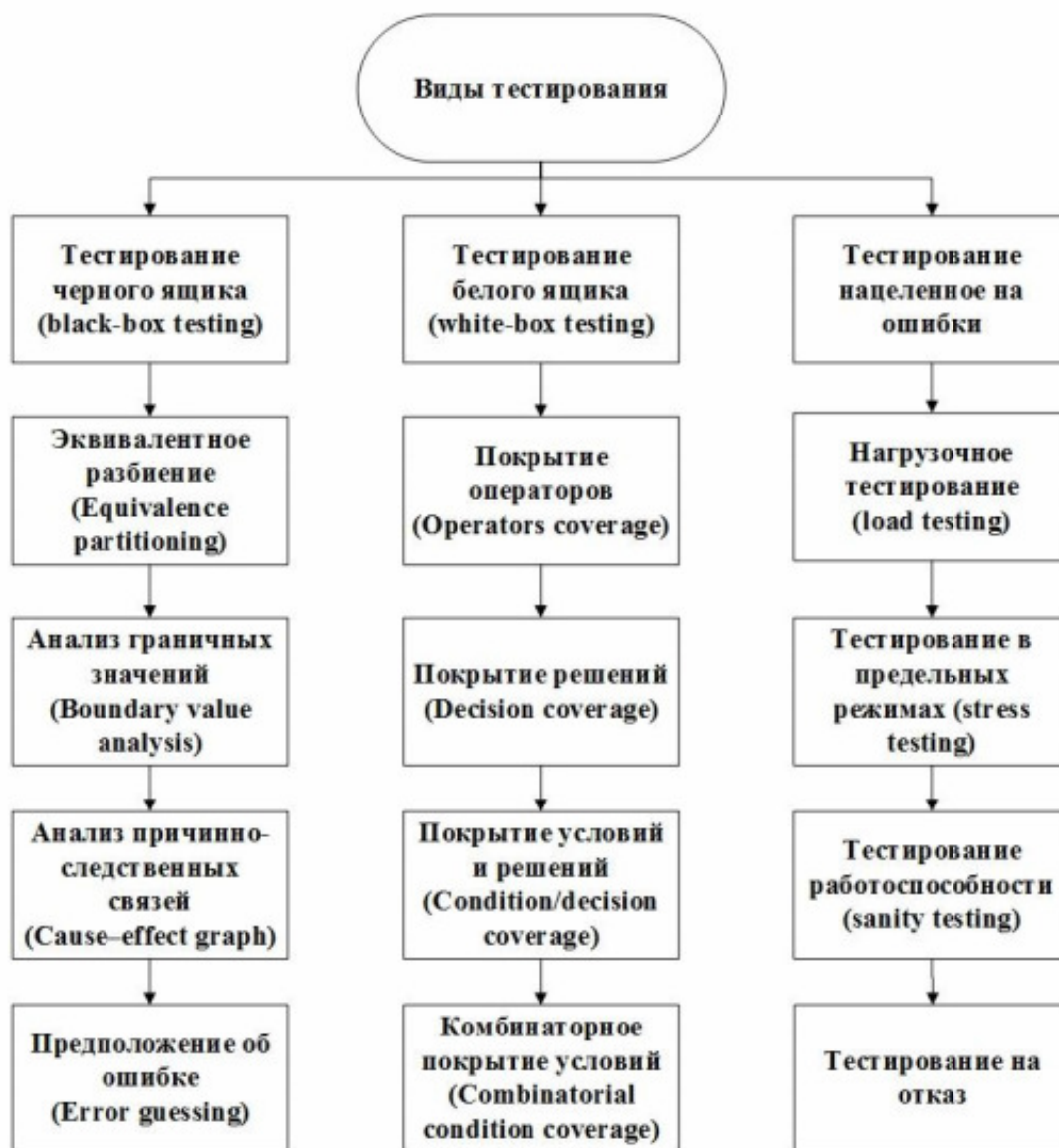


Рис. 1. Виды тестирования

Эффективность методов динамического анализа напрямую зависит от качества и количества входных данных. Обычно эти методы применимы в тех областях, где главным критерием программного обеспечения является время отклика, потребляемые ресурсы и надежность. Такими системами могут являться сервера с базами данных и системы реального времени.

Формальная верификация программ

Формальная верификация основывается на математическом (логическом) моделировании программ и требований к ним. Создается модель – идеализированное описание исследуемого объекта или явления; модель исследуется с применением математических методов; результаты исследования переносятся на реальный объект или явление.

Общая схема формальной верификации показана на рис. 2: создается формальная модель программы; создается формальная модель требований; формально проверяется соответствие модели программы модели требований; на основании результатов проверки делается вывод о соответствии или несоответствии реальной программы реальным требованиям (другими словами, об отсутствии или наличии ошибок в программе).

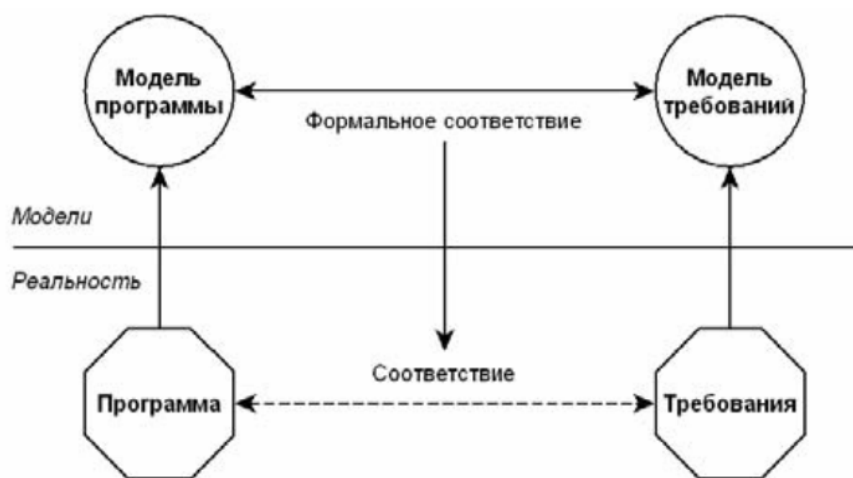


Рис. 2. Общая схема формальной верификации

Для представления моделей программ и моделей требований используются соответственно языки формальной спецификации программ (языки моделирования) и языки формальной спецификации требований.

Методы формальной верификации различаются типами моделей программ (конечные автоматы, сети Петри, размеченные системы переходов), типами моделей требований, отношениями соответствия (эквивалентность, симуляция) и техниками проверки соответствия (исследование пространства состояний, символический анализ, дедуктивный вывод).

Минус формальной верификации – не всегда имеется возможность создать математическую модель. Этот метод можно использовать к тем проверенным участкам, которые можно учесть в формальной модели.

В отличие от статического анализа и формальных методов, динамический анализ позволяет выяснить временные и количественные характеристики программного обеспечения, такие как время выполнения программы в целом и время выполнения её отдельных участков, количество используемых ресурсов (например, занимаемая приложением оперативная память)

Метод динамического исследования также имеет недочеты, прежде всего недостатком этого метода является огромное количество ошибочных срабаты-

ваний. Величина ошибочных срабатываний при использовании новейших инструментов исследования достаточно велика и составляет от 20 до 30 %. Тем не менее динамический анализ – эффективный метод для проверки программного обеспечения.

Список литературы

[1]. *Бурякова Н.А., Чернов А.В.* Классификация частично формализованных и формальных моделей и методов верификации программного обеспечения // Инженерный Вестник Дона. – 2014. – № 4. – С. 129–134

[2]. *Глухих М.И., Ицыксон В.М., Цесько В.А.* Использование зависимостей для повышения точности статического анализа программ // Моделирование и анализ информационных систем. – 2011. – № 4. – С. 68–79

[3]. *Карпов Ю.Г.* MODEL CHECKING. Верификация параллельных и распределенных программных систем. – СПб.: БХВ-Петербург, 2015. – 560 с.

[4]. *Лифшиц Ю.* Верификация программ и темпоральной логики. – СПб., ИТМО, 2005. – С. 3–8

Драган Валерия Владимировна – студент КФ МГТУ им. Н.Э.Баумана, Калуга, 248000, Россия. E-mail:leraspanda@yandex.ru

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИ КОСМИЧЕСКИХ АППАРАТОВ

Каналы связи космических аппаратов. Под космическим аппаратом понимается техническое устройство, которое функционирует с целью выполнения некоторых задач в космическом пространстве. Спектр таких задач в настоящее время очень широк и варьируется от научных исследований до военной разведки, но все они неразрывно связаны со сбором, обработкой, хранением, приемом и передачей различной информации.

Для эффективного и успешного выполнения своих задач космический аппарат должен иметь возможность принимать и передавать информацию между другими космическими аппаратами или наземными объектами по специализированному каналу – каналу космической связи.

Космическая связь – род радиосвязи, осуществляемой при помощи космических объектов, находящихся за пределами атмосферы Земли. Передача информации в таком роде связи осуществляется на радиоволнах УКВ-диапазона.

Современные системы космической связи используют цифровую форму представления сообщений в виде равномерного двоичного кода, которые преобразуются в радиосигнал УКВ-диапазона для передачи по каналу связи. При этом вся передаваемая информация разбивается на небольшие фрагменты фиксированной длины – кадры, которые содержат передаваемые данные и служебные поля [1].

Все кадры, которые передаются по каналам космической связи можно условно разделить на 2 больших класса:

1) Телеметрию – информация, передаваемая с космического аппарата на наземную станцию. Телеметрия содержит информацию, которая собрана с различных датчиков, при этом информация может быть, как служебная, так и научная;

2) Телекоманды – данные и команды управления, передаваемые с наземной станции на космический аппарат.

В настоящее время порядок обмена информацией большинства систем космической связи, основан на международных стандартах и осуществляются с использованием общепринятых протоколов. Кроме того, архитектура систем космической связи строится на основе моделей сетевого взаимодействия, таких как модель OSI (модель взаимодействия открытых систем) или модель TCP/IP [2]. Такой подход позволяет использовать унифицированное оборудование связи и обеспечить большую интеграцию с вычислительными системами, однако расширяет круг возможных абонентов, среди которых могут быть нарушители.

Проблемы безопасности информации. В системах космической связи, как и в других системах обмена и обработки информации, возможно нарушение

ние трех компонентов информационной безопасности: конфиденциальности, целостности, доступности.

Проблема доступности информации связана со спецификой ведения космической связи, и не является предметом данного исследования.

Проблема целостности информации при передаче по каналам связи космических аппаратов во многом связана с наличием различных помех, возникающих в среде передачи радиосигнала УКВ-диапазона. Данные помехи могут быть вызваны рядом факторов, таких как преднамеренное воздействие на канал связи или влияние фона радиоизлучения, создаваемого космическими объектами или наземной инфраструктуры.

Другой причиной нарушения целостности информации может являться модификация информации злоумышленником при помощи внедрения закладок в аппаратуру наземной станции или космического аппарата.

Нарушение целостности передаваемых данных может повлечь за собой серьезные последствия для всей системы связи. Например, в случае приема некорректной команды с наземной станции бортовая аппаратура космического аппарата может выйти из строя, и как результат космический аппарат может навсегда быть утерян в космическом пространстве, что несомненно нанесет материальный ущерб его владельцам [3].

В процессе ведения сеанса связи с космическим аппаратом происходит обмен конфиденциальной информацией, нелегитимный доступ к которой может нанести ущерб интересам владельцев и пользователей космического аппарата.

Поскольку передача информации от космического аппарата производится по достаточно широкой области Земли, то имея на руках необходимое оборудование для приема радиосигнала УКВ-диапазона, и его последующего преобразования в цифровую форму, злоумышленник может получить доступ к конфиденциальным данным. При этом отследить местоположение злоумышленника в ходе перехвата данных не представляется возможным.

В случае применения космического аппарата в исследовательских целях утечка собранных научных данных создает риск упущения экономической выгоды вследствие оформления конкурентами исключительных прав на результат исследовательской деятельности. Кроме того, в случае применения космического аппарата для выполнения государством космической миссии или в целях военной разведки, утечка информации может поставить под угрозу национальную безопасность страны.

Помимо утечки информации по радиоканалу, актуальным является вопрос аутентификации абонента, осуществляющего радиообмен с космическим аппаратом, поскольку прием и исполнение команд от неавторизованного абонента может нарушить штатную работу космического аппарата. Таким образом, отсутствие механизма аутентификации может привести как к утере контроля со стороны легитимных пользователей, так и к полной потере космического аппарата в космическом пространстве, что, в свою очередь, приведет к огромным материальным и временным потерям.

Методы защиты информации. Одним из методов защиты информации передаваемых по каналам связи космических аппаратов является шифрование кадров. В связи с тем, что передаваемые по каналу связи кадры представляют собой фрагменты данных фиксированного размера, то для их шифрования целесообразно применение блочных шифров.

Все алгоритмы шифрования подразделяются на 2 класса: алгоритмы шифрования с закрытым ключом (симметричные алгоритмы) и алгоритмы шифрования с открытым ключом (асимметричные алгоритмы). Каждый из этих классов алгоритмов имеет свои преимущества и недостатки, поэтому выбор алгоритма шифрования во многом зависит от специфики эксплуатации и целей применения космического аппарата.

Симметричное шифрование является наиболее изученным классом шифрования. Данный вид шифрования основан на использовании достаточно простых операций, в связи с чем симметричные алгоритмы просты в реализации, обладают большим быстродействием в сравнении с асимметричными и требуют существенно меньших вычислительных ресурсов[4]. Кроме того, симметричные алгоритмы обеспечивают сопоставимую стойкость на ключах меньшей длины, чем асимметричные алгоритмы. Однако актуальным остается вопрос распределения ключей между абонентами без их компрометации. Таким образом, данные алгоритмы шифрования могут быть применены для защиты информации в каналах связи в тех случаях, когда число абонентов в сети относительно невелико и имеется возможность смены ключа шифрования у абонентов.

Применение асимметричного шифрования позволяет решить проблему распределения ключей между абонентами, поскольку обмен открытыми ключами может производиться непосредственно по незашифрованному каналу космической связи. В результате, данный вид шифрования может применяться в случае нахождения большого числа абонентов в сети космической связи, либо в тех случаях, когда процедура смены ключа симметричного шифрования затруднительна. Однако, при таком подходе возможна реализации атаки «человек по середине», при которой злоумышленник выдает себя за авторизованного абонента и имеет полный контроль над трафиком канала связи.

Другим методом защиты информации является скремблирование – обратимое преобразование цифрового потока без изменения скорости передачи с целью получения свойств случайной последовательности. При этом скремблирование является обратимым процессом, поскольку, применив обратный алгоритм можно восстановить исходное сообщение.

Применение скремблеров позволяет не только обеспечить конфиденциальность информации, но и обеспечить целостность информации передаваемой по каналу связи за счет повышения надежности извлечения приемником информационного сигнала из несущего.

Процесс скремблирования основан на реализации логической операции суммирования по модулю 2 входного и псевдослучайного двоичных сигналов. Основным элементом скремблеров является регистр сдвига с линейной обрат-

ной связью, который выполняет функцию генератора псевдослучайной последовательности [5]. При этом, в зависимости от подхода к инициализации генератора псевдослучайной последовательности, различают 2 типа скремблеров:

- 1) Самосинхронизирующиеся скремблеры;
- 2) Аддитивные скремблеры (скремблеры с установкой).

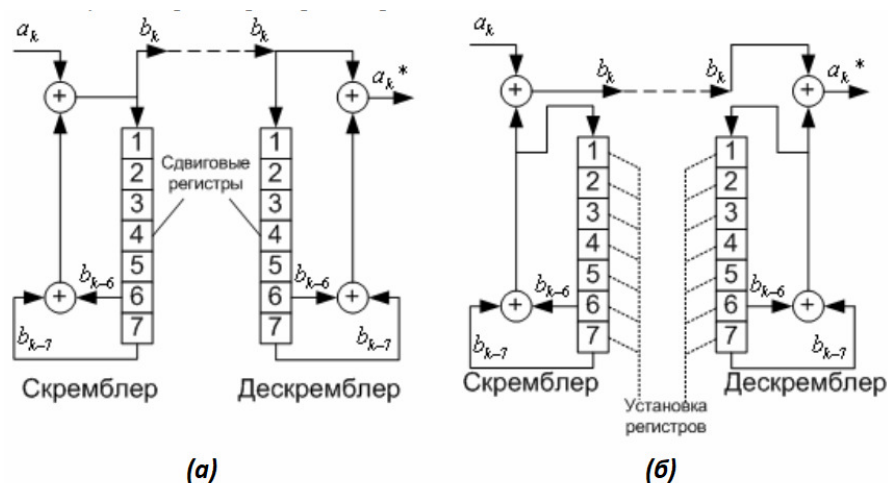


Рис. 1. Схема самосинхронизирующегося (а) и аддитивного (б) скремблирования

Главная особенность самосинхронизирующегося скремблера заключается в том, что он управляется последовательностью бит, которая является результатом скремблирования и передаётся по каналу связи. В связи с этим, достоинством данного типа скремблера является отсутствие необходимости первичной установки генератора псевдослучайной последовательности, поскольку скремблированная последовательность записывается в регистры сдвига на передающей и приемной сторонах, устанавливая их в идентичное состояние. Недостатками данного типа скремблера является наличие свойства размножения ошибок, в случае неправильно принятого бита, а также проблема возникновения периодичности получения выходной последовательности.

В отличие от самосинхронизирующегося скремблера, аддитивный скремблер не управляется скремблируемой последовательностью, поскольку результирующий сигнал не поступает на вход регистра сдвига. В результате такого подхода, аддитивный скремблер лишен недостатков самосинхронизирующегося скремблера, однако возникает задача синхронизации генератора псевдослучайно последовательности на передающей и приемной сторонах.

Список литературы

- [1]. *Пейсахович Д.Г.* Некоторые особенности построения систем передачи телеметрической информации / Д.Г. Пейсахович. – Текст : непосредственный // Молодой ученый. – 2010. – № 8 (19). – Т. 1. – С. 109-112. – [Электронный ресурс] URL: <https://moluch.ru/archive/19/1945/> (дата обращения: 28.10.2020).
- [2.] *Overview of Space Communications Protocols. Informational Report, Issue 3 (Green Book), CCSDS 130.0-G-3.* – Washington, D.C.: CCSDS – 2014. – 43 с. –

[Электронный ресурс] URL: <https://public.ccsds.org/Pubs/130x0g3.pdf> (дата обращения: 28.10.2020).

[3]. *Копик А.* Космические радиолнии. – СПб.: ИД «Вокруг Света», 2007. – №10 (2805) – [Электронный ресурс] URL: <http://www.vokrugsveta.ru/vs/article/5956/> (дата обращения: 28.10.2020).

[4]. *Корниенко А.А., Штанько С.В.* Криптографический протокол защиты информации в радиоканалах сетевых спутниковых систем с использованием асимметричных алгоритмов // Информационно-управляющие системы. – 2006. – №5. – URL: <https://cyberleninka.ru/article/n/kriptograficheskiy-protokol-zaschity-informatsii-v-radiokanalah-setevykh-sputnikovyyh-sistem-s-ispolzovaniem-asimmetrichnyh-algoritmov> (дата обращения: 29.10.2020).

[5]. *Перепелица С.А., Богач Н.В.* Системы и сети связи. Ч.1 Теоретические основы передачи данных в информационных системах. Конспект лекций. – СПб.: Изд-во СПбГПУ, 2008. – [Электронный ресурс] URL: <https://lektsii.org/9-33436.html> / (дата обращения: 28.10.2020).

Кадурин Ярослав Алексеевич – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: mr.cadurin@yandex.ru

АНАЛИЗ ПРОГРАММНЫХ ЛОГОВ

В настоящее время программные логи используются повсеместно. Существует множество сценариев их использования:

- в разработке ПО – для нахождения ошибок и отслеживания состояния;
- в информационной безопасности – для нахождения инцидентов безопасности;
- в мониторинге – для отслеживания состояния объектов.

С ростом информатизации многократно возросло количество генерируемых программных логов. Это приводит к тому, что важные сообщения теряются в общем потоке, а также увеличивается время, необходимое для их анализа и поиска в них интересующих событий [1].

В данной работе рассматриваются программные логи, содержащие действия пользователей в защищаемой АС. В них отражаются все совершаемые пользователем действия, например:

- запускаемое ПО;
- открытие директорий и файлов;
- изменение директорий и файлов;
- посещаемые сайты;
- внесения изменения в системные настройки;
- и другие действия.

Целью данного исследования является анализ походов классификации текстовых данных и определение оптимального с позиции точности и быстродействия для задачи выявления инцидентов безопасности. Инцидентом безопасности называется нежелательное событие, которое способствует значительной вероятности создания серьезной угрозы информационной безопасности. Для его обнаружения на основе программных логов необходимо найти строку, описывающую такое нежелательное событие. При анализе предполагается, что имеется размеченный массив данных, где каждая строка принадлежит либо к классу «инцидент безопасности», либо «безопасное действие».

Самым простым подходом является использование регулярных выражений. Регулярными выражениями называется формальный язык поиска подстрок в строке, основанный на использовании метасимволов для описания шаблона выражения [2]. Данный подход отличается высокой скоростью работы. Однако он имеет крайне низкую точность работы, так как способен находить только заранее описанные в регулярных выражениях строки. Также требуется проведение тщательной экспертизы данных с целью нахождения характерных для каждого класса строк.

Другим подходом является использование простых классификаторов (линейной регрессии, метода опорных векторов или случайного леса). Для их работы необходимо векторизовать текст. Наиболее популярными являются использование модели представления текста как «мешка слов» (Bag of words)

или статистической меры TF-IDF (term frequency – inverse document frequency) [3]. В первом случае каждому имеющемуся в наборе данных слову ставится в соответствие нулевой вектор размерности N с единицей в позиции n , где N – количество слов, а n – номер текущего слова. Во втором – для каждого слова вычисляется вес, который прямо пропорционален частоте употребления этого слова в текущей строке и обратно пропорционален частоте употребления слова во всем тексте. Данный подход показывает низкую или среднюю точность классификации, особенно в ситуации большого числа уникальных слов. Преимуществом данного метода является быстрое действие и простота реализации.

Более выразительными алгоритмами являются нейронные сети. К задаче классификации текстов наиболее часто применяют следующие типы нейронных сетей:

Рекуррентные нейронные сети. Их характерной особенностью является последовательная обработка информации путём переиспользования результата с предыдущего шага [4]. За счёт передачи информации от шага к шагу в сети реализуется «память», что принципиально меняет характер её работы и позволяет лучше анализировать последовательности данных, в которых важен порядок элементов. Данный подход показывает высокую точность классификации текстов, так как способен выявлять сложные взаимодействия между словами, а также другие паттерны, характерные для последовательных данных. Недостатком данного подхода является более низкая по сравнению с другими скорость работы из-за пошаговой обработки данных.

Свёрточные нейронные сети. Данный вид нейронных сетей обычно применяется при анализе графических данных, однако применим и для анализа текстов. Для этого текст рассматривается в виде одноканального изображения с высотой равной единице [5]. Анализ происходит методом скользящего окна. Он позволяет увеличить скорость обработки по сравнению с рекуррентными нейронными сетями за счёт возможности параллелизации вычислений при анализе текста в окне, но как правило за счёт снижения точности распознавания.

Нейронные сети основанные на механизме внимания. Данный вид нейронных сетей позволяет учитывать взаимодействия далеко отстоящих друг от друга символов или слов благодаря расчёту попарных коэффициентов внимания. Также их структура оптимизированная для обширной параллелизации вычислений, что даёт значительный прирост скорости обработки относительно рекуррентных сетей. Сети данной конфигурации дают высокую точность классификации тестов. Главным недостатком является высокое потребление памяти, что ограничивает максимальную длину обрабатываемого текста.

В табл. 1 приведены характеристики рассмотренных методов.

При выборе метода выявления инцидентов безопасности следует помнить о следующих особенностях задачи:

- программные логи представляют собой набор независимых друг от друга коротких строк;

- в программных логах встречается большое количество названий программ, директорий и устройств, что значительно увеличивает число уникальных слов.

Таблица 1.

Характеристики методов анализа текстов

Название метода	Точность классификации	Скорость работы
Регулярные выражения	Крайне низкая	Высокая
Простой классификатор с векторизацией	Низкая или средняя	Высокая
Рекуррентные нейронные сети	Высокая	Низкая
Свёрточные нейронные сети	Средняя	Высокая
Нейронные сети на основе механизма внимания	Высокая	Высокая

Таким образом, использование регулярных выражений для решения данной задачи невозможно из-за слишком большого множества возможных имён в программных логах. Использование простых классификаторов с векторизацией слов также ограничено из-за большого числа уникальных слов. Это ведёт к повышенному потреблению памяти и неспособности классификаторов работать в слишком многомерном пространстве.

Нейронные сети способны справиться с данной проблемой. Так как они обладают значительно лучшей способностью находить закономерности, слова могут быть разделены на токены алгоритмом BPE (byte pair encoding), что позволит им учитывать морфологическую информацию для определения новых имён, которые не встречались в обучающей выборке.

Таким образом, для решения данной задачи лучше всего подходят нейронные сети на основе механизма внимания, так как они обладают наилучшими характеристиками, а их недостаток - сильное потребление памяти при обработке длинных последовательностей, малозначим при решении данной задачи из-за преимущественно короткой длины строк в программных логах.

Список литературы

[1]. *Закирова Г.Ф., Ефимова Ю.В.* Автоматизированная система учета клиентов в компании связи // Теория и практика системной динамики: Материалы конференции VIII Всероссийской конференции (с международным участием). / Ответственный редактор: Олейник А.Г. 2019. С. 84-88.

[2]. *Черемисинов Д.И.* Детерминированная семантика регулярных выражений // Образовательные ресурсы и технологии. – 2016. – №2 (14). – URL: <https://cyberleninka.ru/article/n/determinirovannaya-semantika-regulyarnyh-vyrazheniy> (дата обращения: 10.10.2020).

[3]. *Глазкова А.В.* АВТОМАТИЧЕСКИЙ ПОИСК ФРАГМЕНТОВ, СОДЕРЖАЩИХ БИОГРАФИЧЕСКУЮ ИНФОРМАЦИЮ, В ТЕКСТЕ НА ЕСТЕСТВЕННОМ ЯЗЫКЕ // Труды ИСП РАН. – 2018. – №6. – URL: <https://cyberleninka.ru/article/n/>

avtomaticheskij-poisk-fragmentov-soderzhaschih-biograficheskuyu-informatsiyu-v-tekste-na-estestvennom-yazyke (дата обращения: 10.10.2020).

[4]. *Гринин И.Л.* Разработка, тестирование и сравнение моделей sentimentального анализа коротких текстов // *Инновации и инвестиции*. – 2020. – №6. – URL: <https://cyberleninka.ru/article/n/razrabotka-testirovanie-i-sravnenie-modeley-sentimentalnogo-analiza-korotkih-tekstov> (дата обращения: 11.10.2020).

[5]. *Воробьев Е.В., Пучков Е.В.* Классификация текстов с помощью сверточных нейронных сетей // *Молодой исследователь Дона*. – 2017. – №6 (9). – URL: <https://cyberleninka.ru/article/n/klassifikatsiya-tekstov-s-pomoschyu-svertochnyh-neuronnyh-setey> (дата обращения: 11.10.2020).

[6]. *Vaswani A., Shazeer N., Parmar N. et al.* 2017 Attention Is All You Need (*Advances in Neural Information Processing Systems* 30) – P 5998-6008

Шестопалов Егор Юрьевич – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: shestopalovegor@gmail.com

Молчанов Алексей Николаевич – ассистент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: alexeymolchanov@yandex.ru

А.И. Самохина

АНАЛИЗ ПРОГРАММНЫХ ПРОДУКТОВ ДЛЯ УДАЛЁННОГО КОНТРОЛЯ ИСПОЛНЯЕМЫХ ПРОЦЕССОВ НА РАБОЧИХ СТАНЦИЯХ

Термином «контроль» или «мониторинг» называют работу системы, которая выполняет постоянное наблюдение за работой системы (например, сетевые устройства, настольные компьютеры, серверы или мобильные устройства) в поисках вредоносных, медленных или неисправных подсистем и которая при обнаружении сбоев сообщает о них сетевому администратору посредством уведомлений электронной почты, телефона или специализированного модуля, входящего в состав ПО, предназначенного для мониторинга.

Удалённый мониторинг и управление ИТ-системами осуществляется с помощью локально установленных программных агентов, к которым может обратиться поставщик услуг управления.

Функции включают в себя возможность:

- установить новое или обновить уже присутствующее программное обеспечение удалённо (включая изменения конфигурации);
- обнаруживать новые устройства и автоматически устанавливать агент RMM и настраивать устройство;
- наблюдать за устройствами и программным обеспечением, измерение производительности и диагностика;
- выполнять оповещения и предоставлять отчёты и информационные панели.

Удалённый мониторинг является эффективным решением для управления и контроля нескольких единиц оборудования с одной централизованной консоли.

В настоящее время на рынке программ, выполняющих мониторинг запущенных процессов, существует несколько лидеров, которые превосходят аналогичные программы по многим критериям. Некоторые из них используют терминальный шрифт и интерфейс командной строки, другие решения, наоборот, – выделяются простотой установки и имеют графический интерфейс (включающий в себя таблицы, панели управления, графики и другие инструменты визуализации). Ценовой диапазон также весьма существенно отличается – от бесплатных до решений с дорогой корпоративной лицензией.

Среди лидеров рынка в рассматриваемой области можно выделить следующие программные продукты: **Total Network Monitor 2**, **Observium**, **Nagios**.

Total Network Monitor 2 – это программа для постоянного наблюдения и администрирования локальной сети, отдельных компьютеров, Интернет-ресурсов, сетевых и системных служб. Данное ПО позволяет системным

администраторам вести непрерывное наблюдение за работой локальной сети, постоянно проверяя статус отдельных компьютеров, сетевых и системных служб. Как только Total Network Monitor обнаружит неполадки, он сразу же оповестит об этом администратора, позволяя исправить их прежде чем они перерастут в серьёзные проблемы. Эта программа сохраняет в себе баланс между удобством, заключающимся в наличии графического интерфейса и обширностью функционала.

Одним из основных программируемых компонентов TNM 2 являются мониторы. Это объекты, периодически проверяющие тот или иной аспект работы службы, сервера или файловой системы по заданным значениям. Мониторы гибко настраиваются и отображают состояние контролируемых объектов в реальном времени. При отклонении любых показателей от нормы, монитор выполняет описанный заранее сценарий действий: например, звуковой сигнал, оповещение по e-mail или IM с подробным описанием происшествия, перезагрузка удаленного компьютера, запуск приложения и т.п.

Total Network Monitor записывает состояние всех работающих мониторов в журнал, сохраняя полную информацию о состоянии сети и доступности тех или иных служб. Обратившись к журналу мониторинга, вы всегда можете увидеть историю показаний всех мониторов и список выполненных действий. Эта информация может быть просмотрена непосредственно на панели статистики и в диаграмме активности, либо она может быть экспортирована для построения электронной или печатной версии отчёта. В журналах доступна информация об общем времени работы сети и состоянии всех проверок, что позволяет просматривать полную историю всех возникших проблем или перебоев в работе. Отдельно доступен журнал по всем выполненным действиям. Количество информации, записываемой в журнал, может быть настроено, позволяя печатать как краткие сводки, так и отображать полный технический отчет о каждом событии.

Данный программный продукт способен самостоятельно устранять первичные последствия неполадок (без участия системного администратора) – например, перезагружать отдельные службы или пользовательские устройства, активировать антивирус, дополнять журнал событий новыми записями – все то, что системный администратор должен выполнять вручную.

Стоимость лицензии Total Network Monitor составляет от 2800 рублей и зависит от количества устройств в подконтрольной сети (данные на 2020 год).

Преимущества:

- сравнительно низкая цена;
- дружественный интерфейс;
- легкая установка.

Недостатки:

- отсутствие многопоточности;
- нет возможности обновления;
- отсутствие дашбордов.

Приложение **Observium**, работа которого основана на использовании протокола SNMP, позволяет не только исследовать состояние сети любого масштаба в режиме реального времени, но и анализировать уровень её производительности. Поддерживает широкий спектр типов устройств, платформ и операционных систем, включая Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, Netscaler, NetApp и многие другие. Помимо SNMP собираемая информация может быть дополнена другими способами и протоколами, например, syslog, rancid, unix-agent.

Благодаря проработанному графическому интерфейсу, данное ПО предоставляет системным администраторам большое количество вариантов для настройки – от диапазонов для автообнаружения монтируемых устройств и заканчивая данными протокола SNMP, необходимыми для сбора информации о сети. Observium фиксирует информацию обо всех внутренних датчиках и интерфейсах устройства. Далее, Observium находит все устройства, взаимодействующие с данным с помощью протоколов CDP, LLDP, FDP, или EDP, и осуществляет сбор информации о сетевых «соседях» протоколов маршрутизации, таких как OSPF.

Когда Observium видит соседнее устройство, о котором он еще не знает, он попытается связаться с этим устройством. Если подключение к новому устройству пройдет успешно, процесс автоматического обнаружения будет запущен на нём. Observium будет продолжать исследования, пока вся сеть не будет нанесена на карту. Также данное ПО позволяет получить доступ к данным о технических характеристиках всего оборудования, которое в текущий момент подключено к сети.

После того, как устройство было добавлено в систему, весь его «жизненный» цикл будет отслеживаться в автоматическом режиме. Например, если будет увеличена память или добавится новый датчик или добавится/удалится порт – это все будет обнаружено без ручного вмешательства. Весь сбор статистики поделен на 2 основных процесса: **discovery**, где выполняется основное обнаружение поддерживаемых на данном устройстве датчиков или счетчики и **poller**, где обнаруженные датчики опрашиваются каждые 5-ть минут;

Процессы, в свою очередь, поделены на модули, соответствующие собираемой информации. Основными модули: os, system, ports, mempools, processors, sensors и другие. Фиксируются такие параметры, как ОС, версия, технические характеристики устройства. Также модули поделены на MIB (**Management Information Base**), виртуальная база данных, используемая для управления объектами в сети связи. Информация разнится в зависимости от производителя устройства, типа и доступных датчиков для конкретного устройства.

Преимущества:

- доступна бесплатная версия;
- возможность использования «пороговых» сигналов;
- наличие функций автоматического обнаружения.

Недостатки:

- отсутствие технической поддержки программного продукта;
- сложности в установке;
- корректная работа только в небольших сетях;
- высокая стоимость;
- отсутствие минимального достаточного функционала в бесплатной версии.

Nagios – программа с открытым кодом, предназначенная для мониторинга компьютерных систем и сетей: наблюдения, контроля состояния вычислительных узлов и служб, оповещения администратора в том случае, если какие-то из служб прекращают (или возобновляют) свою работу.

• Управление программой основано на веб-интерфейсе, а её возможности включают в себя:

- Мониторинг сетевых служб (SMTP, POP3, HTTP, NNTP, ICMP, SNMP);
- Мониторинг состояния хостов (загрузка процессора, использование диска, системные логи) в большинстве сетевых операционных систем;
- Поддержка удаленного мониторинга через зашифрованные туннели SSH или SSL;
- Простая архитектура модулей расширений (плагинов) позволяет, используя любой язык программирования по выбору (Shell, C++, Perl, Python, PHP, C# и другие), легко разрабатывать свои собственные способы проверки служб;
- Параллельная проверка служб;
- Возможность определять иерархии хостов сети с помощью «родительских» хостов, позволяет обнаруживать и различать хосты, которые вышли из строя, и те, которые недоступны;
- Отправка оповещений в случае возникновения проблем со службой или хостом (с помощью почты, пейджера, смс, или любым другим способом, определенным пользователем через модуль системы);
- Возможность определять обработчики событий произошедших со службами или хостами для проактивного разрешения проблем
- Возможность организации совместной работы нескольких систем мониторинга с целью повышения надёжности и создания распределенной системы мониторинга;
- Включает в себя утилиту nagiosstats, которая выводит общую сводку по всем хостам, по которым ведется мониторинг.

Что касается обнаружения сетевых аномалий, Nagios автоматически отправляет тревожные уведомления на предустановленный администратором адрес – будь то адрес электронной почты или номер телефона. Стоимость лицензии составляет около \$3000. В течение 60-ти дней доступна бесплатная демо-версия.

Преимущества:

- высокая гибкость;

- полезные шаблоны;
- интеграция с другими приложениями.

Недостатки:

- трудоемкая настройка;
- высокая стоимость;

Из проведённого сравнительного анализа нескольких программных продуктов можно сделать вывод, что для того, чтобы выбрать лучшее решение для удаленного мониторинга и контроля исполняемых процессов, необходимо учитывать потребности компании или частного лица, а также индивидуальные характеристики технического оборудования, на котором оно будет применяться.

Список литературы

- [1]. *Top 10* лучших программ для мониторинга сети в 2020. – URL:<https://www.softinventive.ru/best-network-monitoring-tools/>
- [2]. *Obsevium*: Документация. – URL: <https://docs.observium.org/>
- [3]. *Nagios*. – URL:<https://ru.wikipedia.org/wiki/Nagios>
- [4]. *Network Olympus: Monitoring*. – URL: <https://www.network-olympus.com/ru/monitoring/>

Самохина Анастасия Ильинична – студент КФ МГТУ им. Н.Э. Баумана. E-mail: stasysamdance@gmail.com

АНАЛИЗ СРАВНИТЕЛЬНОЙ ЭФФЕКТИВНОСТИ ПРОГРАММНЫХ ПРОДУКТОВ ТЕСТИРОВАНИЯ УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ

Введение. Уязвимость – это потенциальный способ реализации угрозы информационной безопасности программного обеспечения.

Применение межсетевых экранов, сканеров сетевых уязвимостей и технологии Secure Socket Layer (SSL) не обеспечивает полной безопасности веб-сайта [1]. По оценкам Gartner Group, более 70% атак на веб-приложения происходят на уровне приложений, а не на сетевом или системном уровнях [2]. Программные продукты тестирования уязвимостей веб-приложений или WAS (Web Applications Scanners) помогают своевременно обнаружить большинство уязвимостей и нейтрализовать их в дальнейшем.

Внутреннее устройство веб-приложений. Согласно определению Консорциума безопасности веб-приложений, веб-приложение – это программное обеспечение, исполняемое веб-сервером, отвечающим на запросы динамических веб-страниц посредством сетевого протокола HTTP [3].

Сценарий веб-приложения, располагающийся на веб-сервере, осуществляет взаимодействие с базами данных и иными информационными ресурсами. Поставщики услуг и пользователи веб-приложений могут обмениваться данными независимо от платформы, используя инфраструктуру сети Интернет [4].

Программные продукты тестирования уязвимостей веб приложений. Принцип их действия заключается в поиске уязвимостей путем имитации атак на веб-приложение и анализе его исходного кода. Наилучшей практикой является применение WAS на заключительных этапах разработки веб-приложений.

Различают 2 основных подхода к использованию WAS:

- тестирование в режиме белого ящика (white box testing)
- тестирование в режиме черного ящика (black box testing)

White box testing подразумевает наличие доступа к исходному коду приложения. Black box testing заключается в имитации атак на веб-приложение [5].

В данной статье WAS рассматриваются с позиции black box testing.

Анализ сравнительной эффективности WAS. Было проведено исследование с целью выявления наиболее эффективного среди 5 широко распространенных WAS:

- Vega
- OWASP ZAP
- Nessus
- Acunetix
- Burp Suite

С помощью данных программных продуктов было произведено black box тестирование уязвимостей информационной безопасности следующих заведомо уязвимых веб-приложений:

- demo.testfire.net
- zero.webappsecurity.com
- discuz.net

Статистика результатов тестирования веб-сайта discuz.net по классам уязвимостей в соответствии с классификацией OWASP [6] приведена в табл. 1.

Таблица 1.

Статистика тестирования по классам уязвимостей

Программный продукт	Количество обнаруженных уязвимостей					
	XSS	Cookie	Injection	CSRF	Data Exposure	Access Control
Vega	4	125	1	9	92	2
OWASP ZAP	2	219	5	7	86	4
Nessus	2	518	3	3	15	2
Burp Suite	3	892	3	10	30	7
Acunetix	5	235	5	6	18	1

Исходя из собранных статистических сведений, для каждого из рассматриваемых веб-приложений была разработана модель угроз. Модель угроз для discuz.net приведена в табл. 2.

Таблица 2.

Модель угроз

Угроза	Уязвимость	Вероятность реализации угрозы через заданную уязвимость в течение года	Критичность реализации угрозы через заданную уязвимость
Нарушение работы приложения	XSS	20%	80%
	CSRF	55%	85%
Утечка конфиденциальной информации	Cookie	90%	20%
	Data Exposure	40%	60%
	Injection	10%	75%
Превышение полномочий	Access Control	10%	90%

На основе собранных статистических сведений и разработанных моделей угроз был произведен расчет общего риска информационной безопасности каждого из рассматриваемых веб-приложений. Расчет производился отдельно для каждого из 5 результатов тестирования различными программными продуктами и для соответствующих моделей угроз.

Уровень угрозы по каждой уязвимости был рассчитан по формуле:

$$Th = P(V) \cdot ER,$$

где $P(V)$ – вероятность реализации угрозы через заданную уязвимость в течение года, ER – критичность реализации угрозы через заданную уязвимость.

Уровень угрозы по всем уязвимостям, через которые она может быть реализована, был рассчитан по формуле:

$$CTh = 1 - \prod_{i=1}^n 1 - Th_i,$$

где n – количество уязвимостей, через которые может быть реализована угроза.

Общий уровень угроз, действующий на веб-приложение, был рассчитан по формуле:

$$CThR = 1 - \prod_{i=1}^n 1 - CTh_i$$

Общий риск информационной безопасности веб-приложения был рассчитан по формуле:

$$R = CThR \cdot D,$$

где D – критичность веб-приложения как информационного ресурса. Для расчетов в рамках проведенного исследования, критичность информационного ресурса была принята равной 1000.

Для сравнительного анализа эффективности программных продуктов тестирования уязвимостей веб-приложений на основании рассчитанных значений рисков информационной безопасности был использован критерий Сэвиджа. Результаты анализа приведены в табл. 3.

Таблица 3.

Результаты сравнительного анализа по критерию Сэвиджа

Программный продукт	Y_1	Y_2	Y_3	Y_{min}	Y_{opt}
Vega	-252	-506	-410	-506	-506
OWASP ZAP	-707	0	-405	-707	
Nessus	-565	-1336	0	-1336	
Burp Suite	0	-1038	-1399	-1399	
Acunetix	-1123	-1198	-681	-1198	

Величины Y_i отражают отклонение значения R полученного в результате тестирования каждым из программных продуктов, от максимального. Y_1, Y_2, Y_3 – значения для веб-приложений demo.testfire.net, zero.webappsecurity.com и discuz.net соответственно. Y_{opt} – максимальное значение среди Y_{min} .

Критерий Сэвиджа является оптимальным для решения задачи анализа сравнительной эффективности, поскольку он позволяет выбрать наиболее надежный программный продукт с наименьшим предельным отклонением от максимума по каждому из параметров.

Таким образом, по итогам тестирования и расчета рисков 3 различных веб-приложений Vega является наиболее эффективным программным продуктом на основании критерия Сэвиджа. Рассмотренный в данной статье подход к анализу сравнительной эффективности позволяет осуществить математическое обоснование выбора того или иного программного продукта тестирова-

ния уязвимостей веб-приложения. Гибкость подхода заключается в том, что итоговый результат во многом зависит от выбранного критерия.

Список литературы

[1]. *Grossman J.*, The Five Myths of Web Application Security, White Hat Security, Inc, 2015 – URL: http://index-of.es/Hacking/Web-Application-Vulnerabilities/5_Myths.pdf (дата обращения 13.10.2020)

[2]. *Prescatore J.* Gartner, Computerworld, 2015. – URL: <http://www.computerworld.com/printthis/2005/0,4814,99981,00.html> (дата обращения 15.10.2020)

[3]. *McGraw G.* Building Security In: Software Security, Addison-Wesley Software Security Series, 2016

[4]. *Web Application Security Consortium.* Web Security Glossary. – URL: <http://www.webappsec.org/projects/glossary/> (дата обращения 17.10.2020)

[5]. *Melbourne J., Jorm D.* Penetration Test for Web Applications, SecurityFocus, 2013

[6]. *Web Application Security Consortium.* Threat Classification. – URL: <http://www.webappsec.org/projects/threat/> (дата обращения 18.10.2020)

Теренин Денис Дмитриевич – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: dennisterenin@yandex.ru

Лачихина Анастасия Борисовна – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anastasiaalach73@gmail.com

БЕЗОПАСНОСТЬ ДАТА-ЦЕНТРА: ФИЗИЧЕСКИЙ И ЦИФРОВОЙ УРОВНИ ЗАЩИТЫ

Введение. В современном мире данные-это товар, который требует активной стратегии безопасности центра обработки данных, чтобы управлять ими должным образом. Одно нарушение в системе приведет к хаосу для компании и будет иметь долгосрочные последствия.

Нарушения в доверенных центрах обработки данных, как правило, происходят чаще всего. Чтобы остановить эту тенденцию, поставщики услуг должны принять модель нулевого доверия. От физической структуры до сетевых стоек, каждый компонент должен быть спроектирован с учетом этого.

Модель нулевого доверия рассматривает каждую транзакцию, перемещение или итерацию данных как подозрительные. Это один из новейших методов обнаружения вторжений.

Система отслеживает поведение сети и потоки данных из командного центра в режиме реального времени. Он проверяет всех, кто извлекает данные из системы, и предупреждает персонал или отзывает права у учетных записей, если обнаружена аномалия.

Уровни безопасности и избыточность центров обработки данных. Обеспечение безопасности данных требует контроля безопасности и системных проверок, встроенных слой за слоем в структуру центра обработки данных. От самого физического здания, программных систем и персонала, вовлеченного в повседневные задачи.

Оценка безопасности центра обработки данных начинается с определения местоположения. Дизайн доверенного дата-центра будет учитывать:

- Геологическая деятельность в регионе;
- Высокорисковые отрасли промышленности в этом районе;
- Любой риск затопления;
- Другие риски форс-мажорных обстоятельств.

Можно предотвратить некоторые из перечисленных выше рисков, установив барьеры или дополнительные избыточности в физическом дизайне. Из-за вредного воздействия этих событий на работу центра обработки данных лучше всего вообще избегать их [2].

Проектирование структур, составляющих центр обработки данных, должно снизить любые риски контроля доступа. Ограждение по периметру, толщина и материал стен здания, а также количество входов в него. Все это влияет на безопасность центра обработки данных.

Некоторые ключевые факторы также будут включать в себя:

- Здания нуждаются в более чем одном поставщике как телекоммуникационных услуг, так и электроэнергии;
- Дополнительные системы резервного питания, такие как ИБП и генераторы, являются критической инфраструктурой;

– Использование ловушек для людей. Это включает в себя наличие воздушного шлюза между двумя отдельными дверями, причем аутентификация требуется для обеих дверей;

– Отдельные системы поддержки от белых пространств позволяют уполномоченным сотрудникам выполнять свои задачи. Это также останавливает техников по техническому обслуживанию и техническому обслуживанию от получения неконтролируемого входа.

Любое устройство, будь то сервер, планшет, смартфон или ноутбук, подключенный к сети дата-центра, является конечной точкой. Центры обработки данных предоставляют места в стойках и клетках клиентам, чьи стандарты безопасности могут быть сомнительными. Если клиент неправильно защитит сервер, весь центр обработки данных может оказаться под угрозой. Злоумышленники собираются попытаться воспользоваться незащищенными устройствами, подключенными к интернету. Например, большинство клиентов хотят получить удаленный доступ к распределительному блоку питания (PDU), чтобы они могли удаленно перезагрузить свои серверы. Безопасность является серьезной проблемой в таких случаях [1].

Аудиты могут варьироваться от ежедневных проверок безопасности и физических пошаговых инструкций до ежеквартальных проверок PCI и SOC. Физические аудиты необходимы для проверки соответствия фактических условий отчетным данным.

Стандарты безопасности центров обработки данных. Существует тенденция к повышению безопасности услуг передачи данных и стандартизации безопасности центров обработки данных.

В подтверждение этого Uptime опубликовало систему классификации уровней для центров обработки данных. Система классификации устанавливает стандарты для элементов управления центра обработки данных, которые обеспечивают доступность. Поскольку безопасность может влиять на время безотказной работы системы, она является частью их стандарта классификации уровней [3].

Существует четыре уровня, определенных системой. Каждый уровень соответствует бизнес-потребностям, которые зависят от того, какие данные хранятся и управляются.

Первый и второй уровни, рассматриваемые как тактические службы, будут иметь только некоторые из функций безопасности, перечисленных в данной работе. Они дешевы и используются компаниями, которые не хотят иметь доступ к своим данным в режиме реального времени и которые не пострадают финансово из-за временного сбоя системы.

Они в основном используются для хранения данных за пределами объекта.

Третий и четвертый уровни имеют более высокий уровень безопасности. Они имеют встроенные резервные копии, которые обеспечивают бесперебойную работу и доступ. Предоставление критически важных услуг для компаний, которые знают цену ущерба репутации, создаваемого

перерывом в обслуживании. Эти средства обработки данных в реальном времени обеспечивают самые высокие стандарты безопасности.

Все больше и больше компаний переносят свои критические рабочие нагрузки и услуги на размещенные серверы и инфраструктуру облачных вычислений. Центры обработки данных-главная мишень для злоумышленников.

Список литературы

[1]. *Казарин О.В.* Надежность и безопасность программного обеспечения : учебное пособие для вузов / О.В. Казарин, И. Б. Шубинский. – М.: Издательство Юрайт, 2020. – 342 с.

[2]. *Опарин С.Г.* Архитектурно-строительное проектирование : учебник и практикум для вузов / С.Г. Опарин, А.А. Леонтьев. – М.: Издательство Юрайт, 2020. – 283 с.

[3]. *Северцев Н.А.* Введение в безопасность : учебное пособие для академического бакалавриата / Н.А. Северцев, А.В. Бецков. – 2-е изд., перераб. и доп. – М.: Издательство Юрайт, 2019. – 177 с.

Бандурина Екатерина Михайловна – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: bandurinakatya7@yandex.ru

Ерохин Илья Игоревич – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: drleiter@rambler.ru

ИЗМЕРЕНИЕ КИБЕРФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ В ПРОМЫШЛЕННЫХ СИСТЕМАХ УПРАВЛЕНИЯ С ПОМОЩЬЮ СТРАТЕГИЙ АТАК С МИНИМАЛЬНЫМИ УСИЛИЯМИ

Введение. За последние годы промышленные системы управления (СУ) стали привлекательной мишенью для злоумышленников. Причины этого включают в себя в основном их повышенную связь с внешним миром, их недостаточную готовность к кибератакам и огромное влияние, которое эти атаки могут оказать на многие аспекты современного общества. Будучи жизненно важной частью критически важной национальной инфраструктуры, защита СУ от киберугроз становится приоритетной задачей, поскольку их компрометация может привести к множеству различных проблем: от сбоев в обслуживании и экономических потерь до угрозы природным экосистемам и угрозы человеческой жизни [1].

Идентификация критических узлов не только позволяет аналитикам определить метрику для измерения уровня безопасности системы, но и предоставляет полезную информацию, которая может быть использована для принятия решения о том, как и где повысить безопасность, а также для добавления избыточных и резервных компонентов.

Основные критерии измерения киберфизической безопасности систем управления. Данный подход основан на графах и/или гиперграфах для моделирования сред СУ с несколькими перекрывающимися мерами безопасности, а также на методах MAX-SAT для оптимального вычисления критических узлов сети. В данную технику также включен стандарт META4ICS, основанный на Java анализатор метрик безопасности для СУ.

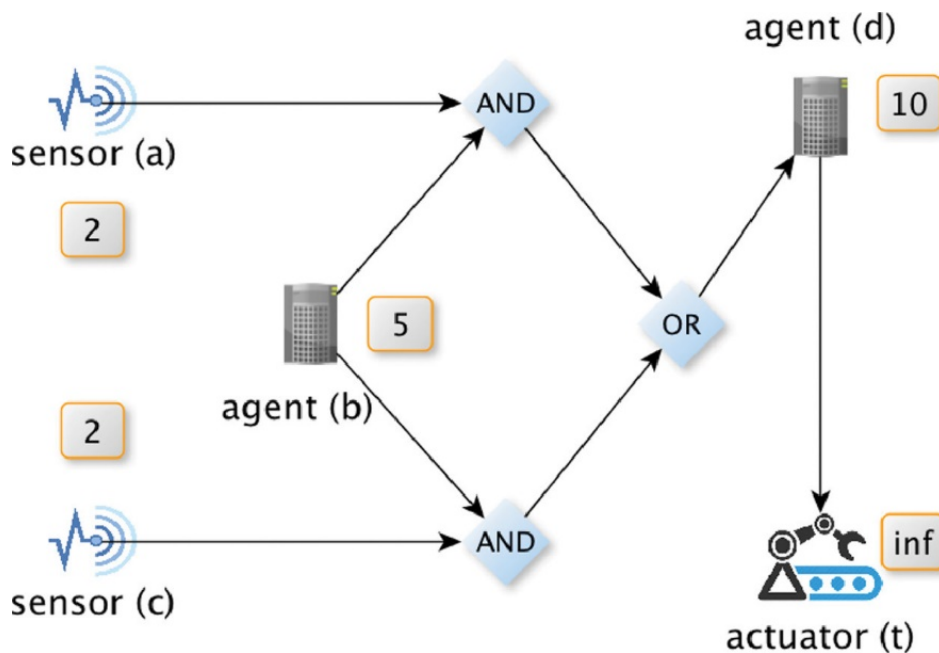


Рис. 1. Базовый случай-взвешенный И/ИЛИ граф

На рис. 1 показан простой график, включающий пять компонентов CPS в виде атомарных узлов, а именно двасенсора (a и c), два программных агента (b и d) и один исполнительный механизм (t). График выглядит следующим образом: привод t зависит от выхода программного агента d , например программируемого логического контроллера. Агент d , в свою очередь, имеет две альтернативы для правильной работы; он может использовать либо показания датчика a и выходные данные агента b вместе, либо выходные данные агента b и показания датчика c вместе взятые.

Теперь предположим, что каждый компонент логического контроллера также имеет ассоциированное значение (или вес), которое представляет его компромиссную стоимость (т.е. усилия злоумышленника), где inf означает бесконечность. Учитывая эти компромиссные издержки, попытаемся ответить на вопрос: какие узлы должны быть скомпрометированы, чтобы нарушить работу привода tc с минимальными усилиями (затратами) для атакующего? Другими словами, какова стратегия атаки с наименьшими усилиями для отключения привода t ?

Этот базовый пример включает в себя множество вариантов атаки, однако только один из них минимален. Например, злоумышленник может скомпрометировать узел d и, таким образом, целевой узел t будет успешно отключен от графика. Другим вариантом является возможность скомпрометировать узел bc более низкой стоимостью, а так как узел b связывает оба узла AND, они будут нарушены и последовательно узел OR, что в свою очередь повлияет на узел d и, наконец, на узел t . Однако с точки зрения затрат оптимальной стратегией для злоумышленника в этом случае является компрометация узлов a и c общей стоимостью. С точки зрения защиты можно принять эту минимальную стоимость как показатель, который отражает уровень безопасности системы, которую пытаются защитить [3].

Хотя в некоторых случаях это весьма полезно, назначение индивидуальных затрат на каждом узле может охватывать только те меры киберфизической безопасности, которые применяются независимо к каждому компоненту СУ [4]. Например, этот метод может зафиксировать, что датчики a и c защищены огороженными участками, каждый из которых имеет стоимость 2, но он не может смоделировать, что оба датчика защищены одной огороженной областью со стоимостью 2. В последнем случае усилия (затраты) злоумышленника, необходимые для компрометации механизма безопасности, должны рассматриваться только один раз. Это приводит к более общему случаю, как показано на рис. 2, где проблема двоякая: с одной стороны, необходимо определить критические компоненты, которые могут отключить цель от её зависимостей в графе И/ИЛИ, а с другой стороны, минимизировать усилия атаки, наложенные мерами безопасности, которые совместно применяются для защиты нескольких компонентов СУ одновременно.

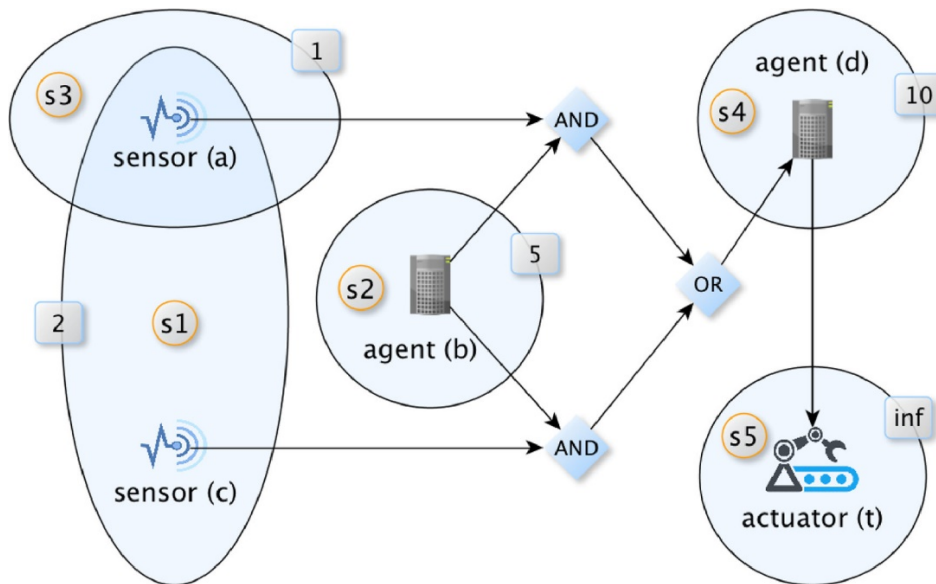


Рис.2. Общий случай-перекрывающиеся взвешенные меры

В этом втором сценарии датчики *a* и *c* защищены одним и тем же экземпляром меры безопасности *S1* (например, огороженной территорией). Таким образом, стоимость обхода *S1* для компрометации датчика *a*, датчика силы обоих датчиков равна 2. Однако датчик *a* также защищен мерой безопасности *S3* (например, запертым контейнером). Как следствие, компрометация датчика *a* будет означать обход как защитных мер *S1*, так и *S3*. Поэтому наилучшей стратегией в данном случае является компрометация мер безопасности *S1* и *S3*, включающих критические узлы *a* и *c*, с общей стоимостью 3 [2].

Заключение. Таким образом, на основании двух базовых примеров, помогающий ярко проиллюстрировать проблему, можно сделать вывод, что идентификация критических компонентов в больших сценариях с несколькими перекрывающимися элементами управления безопасностью становится значительно сложнее. С точки зрения теории графов второй подход ищет минимальную взвешенную вершину, вырезанную в И/ИЛИ графах. В то время как хорошо известные алгоритмы, такие как Max-flow или Min-cut и их варианты его могут быть использованы для оценки такой метрики над графами или графами в полиномиальное время, их использование для общих И/ИЛИ графов не очевидно и не тривиально, поскольку они могут не улавливать лежащую в основе логическую семантику графа. В этом смысле второй подход направлен на оказание более полезной поддержки в принятии решений по вопросам безопасности, расстановки верных приоритетов для планирования смягчения последствий и повышения устойчивости среды СУ.

Список литературы

[1]. Казарин О.В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. – М.: Издательство Юрайт, 2020. – 342 с.

[2]. *Каракеян В.И.* Надзор и контроль в сфере безопасности : учебник для вузов / В.И. Каракеян, Е.А. Севрюкова ; под общ. ред. В.И. Каракеяна. – М.: Издательство Юрайт, 2020. – 397 с.

[3]. *Плескунов М.А.* Прикладная математика. Задачи сетевого планирования : учебное пособие для вузов / М. А. Плескунов ; под научн. ред. А.И. Короткого. – 2-е изд. – М.: Издательство Юрайт, 2020. – 93 с.

[4]. *Северцев Н.А.* Системный анализ теории безопасности : учебное пособие для вузов / Н.А. Северцев, А.В. Бецков. – 2-е изд., перераб. и доп. – М.: Издательство Юрайт, 2020. – 456 с.

Бандурина Екатерина Михайловна – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: bandurinakatya7@yandex.ru

Ерохин Илья Игоревич – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: drleiter@rambler.ru

Е.В. Поддубная

ИНФОРМАЦИОННАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ ЧЕЛОВЕЧЕСКИМИ РЕСУРСАМИ ПРЕДПРИЯТИЯ ТРАНСПОРТИРОВКИ ГАЗА

В работе рассматривается разработка информационной модели процесса обеспечения человеческими ресурсами (ЧР) предприятия осуществляющего транспортировку газа, с помощью которой осуществляется поддержка принятия решений путем представления процесса обеспечения предприятия человеческими ресурсами [1].

Свойства данного процесса представлены в виде предлагаемой информационной модели:

$$A = \{I, Fc, Ce(t,e), Cp(t,e), Cu(u), eP, es, ec, \delta\}, \quad (1)$$

где I – параметры анализируемого периода времени, на протяжении которого осуществляется обеспечение предприятия ЧР; Fc – представление предприятия на верхнем уровне в виде составного объекта, в который входят все остальные, входящие в него простые и составные объекты; $Ce(t,e)$ – функция стоимости ЧР e в момент времени t ; $Cp(t,e)$ – функция величины штрафа (дополнительной оплаты труда) сверхурочного использования ЧР в момент времени t ; $Cu(u)$ – функция цены стоимости услуги определенного типа u ; ep, es, ec – пороговые значения выявления несоответствия плану, выявления утечки и определения рентабельности мероприятия соответственно, которые задаются лицами, принимающими решения; δ – коэффициент штрафа за каждую не предоставленную услугу в соответствии с планом.

Объекты предприятия могут быть простыми и составными. Простые объекты – это те, которые рассматриваются как конечный представитель услуг и потребитель ЧР, который не может быть разделен. Составной объект – объект, состоящий из вложенных в него объектов, который при этом сам может пользоваться ЧР, а также в объемы его затрат входят затраты вложенных в него объектов. При этом он также может предоставлять какие-то услуги и или же в объемы предоставляемых им услуг входит совокупность объемов, производимых вложенными в него подобъектами [2].

Простой объект предприятия представляется в виде следующей информационной модели, кортежа, показанного в формуле:

$$F_S = \{n_F, O(u,e), Pp(t,u), P_R(t,u), R, E_H(t,u,e), E_M(t,e), E'E(t,u,e)\}, \quad (2)$$

где n_F – наименование объекта или иная строка, идентифицирующая его; $O(u,e)$ – производительность объекта, определяющая для каждого типа услуги и объемы потребляемых ЧР заданного типа e , необходимых для предоставления единицы продукции; $Pp(t,u)$ – функция производственного плана для объекта предприятия, которая возвращает количество

предоставленных услуг u -го типа в момент времени t (Данные могут быть взяты из файла или БД, аналогично тому, как берутся данные использования из табеля рабочего времени); $P_R(t,u)$ – реальные данные об объемах предоставленных услуг определенного типа и в момент времени t ; R – примененное к данному объекту мероприятие, описывающее обновленные параметры объекта предприятия и его стоимость (если на одном объекте выполняется несколько мероприятий, в данной работе на текущий момент они должны быть представлены в виде одного, а их эффекты и стоимость суммироваться); $E_H(t,u,e)$ – функция получения рассчитанных данных ожидаемого использования ЧР с текущими характеристиками данного объекта.

Функция ожидаемого использования ЧР с применением новых характеристик данного объекта показана в формуле:

$$E'E(t,u,e) = E'_c(t,e) + E'_o(t, O'(u, e)), P'_p(t,u) \quad (3)$$

Кортеж составного ОМП дополняется ещё множествами F_{si} и F_{sv} вложенных простых и составных объектов соответственно (для простого объекта данные множества являются пустыми), а также функцией $E_s(t,e)$ – функция получения суммы измеренных данных использования ЧР вложенными подобъектами данного объекта [3]. В итоге кортеж модели составного объекта показан в формуле:

$$FE = \{nF, F_s, FC, O(u,e), Pp(t,u), P_R(t,u), R, EE(t,u,e), E_m(t,e), E'E(t,u,e), E_s(t,e)\}, \quad (4)$$

Причем, функции $Pp(t,u)$ и $P_R(t,u)$ для составного объекта могут не задаваться, если он ничего не предоставляет, а только содержит в себе вложенные объекты.

Множества данных об использовании ЧР представлены в виде следующей информационной модели (кортежа), показанной в формуле:

$$E = \{S, D\}, \quad (5)$$

где $S = \langle s_i, \dots, S_k \rangle$, где S_k – это одна из множества k характеристик источника данных, откуда они получены, необходимых для анализа данных, например тип ЧР, объемы, использования которых описывают эти данные, интервал сбора данных из данного источника, наименование объекта и т.п. (единицы измерения, интервал измерения (1 мин., 15 мин., 1 час), множители, тип данных и др.; $D = \langle d_i, \dots, d_l \rangle$, где d_i – это один из l элементов данных в данном множестве.

На текущий момент данная модель имеет следующие ограничения:

- в данной модели на текущий момент не рассматриваются вторичные ресурсы;
- данная модель работает только с историческими данными использования ЧР объектами предприятия;
- в данной модели не учитываются ряд других параметров, например,

трудоемкости использования нового оборудования, что также повлияет на срок его окупаемости, а также может повлечь дополнительные затраты.

Список литературы

[1]. *Пожарницкая О.В., Цибульникова М.Р.* Кадровая стратегия как фактор устойчивого развития нефтегазового сектора // Современные проблемы науки и образования. – 2014. – № 2. – URL: www.science-education.ru/116-12267 (дата обращения: 26.10 2020).

[2]. *Балаба А.В.* Человеческие ресурсы как фактор конкурентоспособности предприятия // Компетентность. – 2012. – № 2/93. – С. 46–49.

[3]. *Бурков В.Н., Панова Л.Н., Шнейдерман М.В.* Получение и анализ экспертной информации. – М.: Изд-во Института проблем управления, 1981. – 340с.

Поддубная Екатерина Викторовна – аспирант КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: viskano@rambler.ru

ИССЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ СИСТЕМЫ ТЕХНИЧЕСКОЙ ПОДГОТОВКИ ПРОИЗВОДСТВА

Методы защиты технической подготовки производства. Деятельность предприятия по развитию его материально-технической базы, организации производства, труда и управления представляет собой техническую подготовку производства [1].

Для того, чтобы провести исследование защищенности системы технической подготовки производства, необходимо провести анализ моделиданной автоматизированной системы. На рис. 1 представлена модель автоматизированной системы технической подготовки производства.

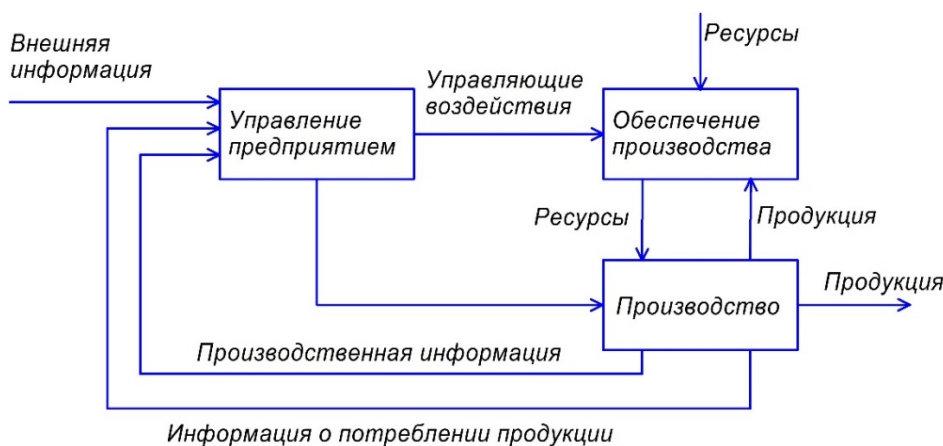


Рис. 1. Модель автоматизированной системы
технической подготовки производства

Как видно из рисунка, ключевыми элементами данной системы являются производственная и внешняя информация.

Для определения комплекса методов, необходимых для организации защиты технической подготовки производства необходимо провести анализ защищенности рассматриваемой системы.

Наиболее критичными уязвимостями являются:

- отсутствие формальной модели управления доступом;
- отсутствие криптографических механизмов защиты информации;
- отсутствие механизмов поддержания целостности;
- отсутствие механизмов резервного копирования.

Через данные уязвимости могут быть реализованы такие угрозы как несанкционированный доступ к информации, несанкционированное изменение и уничтожение информации.

Одним из наиболее важных свойств информационной системы предприятия является безопасность её информационных ресурсов. Исторически сферой защиты информации являлось противодействие намеренному нарушению её конфиденциальности, то есть несанкционированному копированию, прочтению, замене, уничтожению и т.п. Основными инструментами при этом бы-

ли шифрование, перекрытие каналов утечки информации и контроль доступа к информационной инфраструктуре [2].

Уровень защищенности системы принято выражать уровнем риска информационной безопасности.

Риск информационной безопасности (ИБ) – это потенциальная возможность реализации угроз ИБ через уязвимости инфраструктуры с причинением ущерба предприятию.

Величина риска определяется как произведение вероятности наступления негативного события на размер ущерба.

Под вероятностью наступления события понимается произведение вероятности реализации угрозы информационной безопасности на уязвимость информационной безопасности, выраженной в качественной или количественной форме [3].

Для проведения анализа рисков составлена табл. 1, в которой идентифицированы угрозы и рассчитаны вероятности негативных событий.

Таблица 1.

Вероятность негативных событий

Угроза (вероятность угрозы)	Уязвимости (суммарная величина уязвимостей)	Вероятность события
1. Несанкционированный доступ к информации (высокая)	Отсутствие формальной модели управления доступом; отсутствие криптографических механизмов защиты информации. (высокая)	Высокая
2. Несанкционированное изменение информации (средняя)	Отсутствие формальной модели управления доступом; отсутствие механизмов целостности. (высокая)	Высокая
3. Несанкционированное уничтожение информации (средняя)	Отсутствие формальной модели управления доступом; отсутствие механизмов резервного копирования. (высокая)	Высокая

В табл. 2 показаны степени ущерба для автоматизированной системы технической подготовки производства при реализации конкретных угроз.

Таблица 2.

Степени ущерба для информационной системы

Угроза	Степень ущерба
1. Несанкционированный доступ к информации	Высокая
2. Несанкционированное изменение информации	Высокая
3. Несанкционированное уничтожение информации	Высокая

Результат анализа рисков информационной безопасности для системы технической подготовки производства показан в табл. 3.

Величина риска

Событие (вероятность события)	Размер ущерба от события	Величина риска
1. Несанкционированный доступ к информации (высокая)	Высокий	Высокая
2. Несанкционированное изменение информации (высокая)	Высокий	Высокая
3. Несанкционированное уничтожение информации (высокая)	Высокий	Высокая

Вывод. Таким образом, противодействие угрозам несанкционированного доступа к информации, несанкционированного изменения и уничтожения информации, связанной с технической подготовкой производства, является одной из ключевых задач по обеспечению безопасности на любом предприятии. Для противодействия этим угрозам необходимо применять организационные и технические методы. К этим методам относятся: пропускной режим, охрана, должностные инструкции персоналу по вопросам информационной безопасности, программное обеспечение, обеспечивающее механизмы формальной модели управления доступом, криптографические механизмы защиты информации, механизмы поддержания целостности и механизмы резервного копирования.

Список литературы

[1]. *Золотогоров В.Г.* Организация и планирование производства: практическое пособие. – М: Изд-во ФУАинформ, 2017. – 527 с.

[2]. *Лачихина А.Б., Петраков А.А.* Целостность данных как критерий оценки защищенности ресурсов корпоративных информационных систем. // Вопросы радиоэлектроники. – 2019. – № 11. – С. 77-81.

[3]. *Мельников В.П.* Информационная безопасность и защита информации. – М.: Изд-во Издательский центр «Академия», 2018. – 336 с.

Михаил Дмитриевич Романкин – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: romankinmike@gmail.com

Лачихина Анастасия Борисовна – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anastasia_lach73@gmail.com

ИССЛЕДОВАНИЕ МЕТОДОВ КОНТРОЛЯ МОБИЛЬНЫХ УСТРОЙСТВ НА БАЗЕ ANDROID

С каждым годом смартфоны становятся более производительными. Они все быстрее передают данные, делают более качественные фотографии и видео, имеют более емкие запоминающие устройства, наполняются огромным количеством приложений. И самое главное, они имеют доступ к все более критичной информации из нашей жизни – кредитным картам, информации о состоянии здоровья, местоположению и т.д. [1].

Вне зависимости от модели автоматизированной системы предприятия, существует угроза кражи данных с помощью фотофиксации каких-либо документов, которые составляют коммерческую или государственную тайну (фото монитора компьютера, бумажных носителей и т.д.).

Можно сделать вывод, что как бы предприятия ни старались выстроить свой технический периметр безопасности, они всегда будут подвержены инсайдерским атакам со стороны персонала, чему в наше время способствуют мобильные устройства, которые имеют полный набор технических возможностей для их осуществления.

Инсайдерские угрозы — это вредоносные для организации угрозы, которые исходят от людей внутри организации, таких как работники, бывшие работники, подрядчики или деловые партнеры, у которых есть информация о методах безопасности внутри организации, данных и компьютерных системах.

Чтобы правильно выбрать способы борьбы с угрозами, связанными с мобильными устройствами, необходимо определить типы нарушителей, с которыми необходимо бороться. Условно их можно разделить на три группы:

- Использование мобильного устройства в личных целях;
- Небрежность и низкая грамотность при использовании устройств;
- Намеренное киберпреступление с помощью мобильного устройства.

Существующие методы контроля мобильных устройств:

Ограничение на использование мобильных устройств на работе

Некоторые компании (особенно связанные с гостайной) практикуют сбор мобильных телефонов на проходных. Это, пожалуй, самый радикальный способ защиты и при строгом контроле он может быть эффективным.

Использование MDM/EMM решений

MobileDeviceManagement, MDM – программное обеспечение для работы с корпоративными системами при помощи мобильных устройств [2].

Такие решения ограничивают возможность удаленного доступа к корпоративным информационным системам только для определенных устройств. Этот подход позволяет защитить информацию, но не спасает на 100% от IT-рисков типа распространения вредоносного программного обеспечения (ПО), передачи информации на телефон или с телефона в режиме USB.

Комплексный контроль

Оптимальный подход – использовать компоненты DLP-систем. DLP-система (от англ. DataLeakPrevention) это специализированное ПО, которое защищает организацию от утечек данных. Данная технология – это не только возможность блокировать передачу конфиденциальной информации по различным каналам, но и инструмент для наблюдения за ежедневной работой сотрудников, который позволяет найти слабые места в безопасности до наступления инцидента [3].

Использование подавителей мобильного сигнала

В России не запрещено использовать специальные подавители сотового сигнала, но их нужно зарегистрировать (вопросом занимается Государственная комиссия по радиочастотам). Эти устройства создают плотные помехи на выбранной частоте (3G, LTE, 5G). Человек не сможет пользоваться сотовой сетью для передачи данных. Однако это должны делать специалисты и крайне аккуратно, т.к. есть риск полностью заблокировать связь, что вызовет недовольство и подозрения, а также навредит бизнес-процессам компании

Предложение по способу контроля функционала мобильного телефона

Для минимизации данных угроз необходимо модифицировать организационную и техническую части. С технической стороны необходимо модифицировать систему управления доступом. А именно, интегрировать в нее возможность управления функционалом мобильных устройств персонала, которые в данный момент находятся на территории предприятия. Т.е. после предъявления электронного пропуска считывателю на контрольно-пропускном пункте, управляющий сервер регистрирует присутствие сотрудника на рабочем месте (предприятии) и связывается с его мобильным устройством с помощью защищенного интернет соединения. В свою очередь на мобильном устройстве установлена специальная программа, которая работает с правами администратора устройства в фоновом режиме, блокируя при необходимости доступ к камере и интернету отдельным приложениям удаленно. Сервер периодически опрашивает устройство для проверки активности программы, и, если связь с устройством будет утрачена, сервер информирует службу информационной безопасности о данном событии.

С точки зрения совершенствования организационной системы необходимо задокументировать данную систему:

- проинформировать сотрудника о том, что планируется использовать данную систему;
- взять письменное соглашение работника;
- ввести дополнительные штрафы для работников контрольно-пропускного пункта, если вследствие их халатности на предприятие удалось пронести незарегистрированное в данной системе устройство;
- ввести дополнительные методы поощрения для работников контрольно-пропускного пункта за пресечение проноса незарегистрированных устройств;

— ввести дополнительные штрафы за несоблюдение условий нахождения внутри защищаемого периметра;

— в качестве мотивации использования данной системы для работников, создать отдельное помещение для полноценного использования своих мобильных устройств с ограниченным временем пребывания в данной комнате. После окончания выделенного времени доступ к функционалу устройства блокируется до конца рабочего дня.

Список литературы

[1]. *Контроль* мобильных устройств: четыре подхода к решению большого вопроса – [Электронный ресурс] – URL: <http://www.iksmedia.ru/articles/5658606-Kontrol-mobilnyx-ustrojstv-chetyre.html#ixzz6cBZ35ai0> (дата обращения 28.10.2020)

[2]. *Управление* мобильными устройствами – [Электронный ресурс] – URL: [https://www.tadviser.ru/index.php/Mobile_Device_Management_\(MDM\)](https://www.tadviser.ru/index.php/Mobile_Device_Management_(MDM)) (дата обращения 28.10.2020)

[3]. *DLP-система* – что это такое и зачем нужна? – [Электронный ресурс] – URL: <https://falcongaze.com/ru/pressroom/publications/dlp-sistemy/what-is-dlp.html> (дата обращения 28.10.2020)

Еськов Егор Сергеевич – студент ИУК6-111 КФ МГТУ им. Н.Э. Баумана. E-mail: egor.esckov@yandex.ru

КУЛЬТУРА ОБОРОТА ПЕРСОНАЛЬНЫХ ДАННЫХ РОССИЙСКОГО СЕГМЕНТА ИНТЕРНЕТА

«Оператор сознался в продаже записей пользовательских данных», «Хакерами были взломаны аккаунты пользователей торгового сайта», «Вся информация, находящаяся на сервере, была получена мошенниками» – это лишь несколько заголовков из уже привычных всем новостей.

Молодой и экономически активный гражданин, особенно если он проживает в крупном городе, вполне может в течение года по статистике 10–20 раз и даже чаще оставлять свои персональные данные в различных государственных органах, на бизнес-платформах и в социальных проектах, говорит Андрей Арсентьев, аналитик ГК InfoWatch.

По оценке «Левада-центра», около 60% взрослых россиян активно пользуются социальными сетями, при этом многие зарегистрированы сразу на нескольких популярных ресурсах. Таким образом, на эти платформы также регулярно передаются массивы пользовательских данных.

Кроме того, с каждым годом всё больше персональных данных передается на платформы интернета вещей. Например, источниками таких данных служат фитнес-браслеты и устройства умного дома.

Если оставить за скобками запись разговоров абонента, то сейчас бизнес и телеком, и банки, и соцсети, и интернет-сервисы собирают сотни килобайт данных о человеке в день, говорит партнер КПМГ Алена Дробышевская.

Как правило, разрешение на сбор, обработку и использование любой нашей информации мы даем в тот момент, когда «подписываемся» под лицензионным соглашением приложения или интернет-сервиса. Безопасен ли такой, практически неконтролируемый, сбор данных? Естественно, нет. Более того, обеспечение приватности данных пользователя и защита его от взломов и утечек – не менее важная задача для современных защитных решений, чем защита от вирусов или фишинга [1].

В сложившейся ситуации хорошо видны несколько фундаментальных противоречий между тремя основными объектами современного информационного общества:

— Обычный человек не хочет, чтобы государство или коммерческие организации следили за каждым его шагом, но при этом желает пользоваться бесплатными сервисами, невозможными без сбора данных.

— Бизнес хочет максимально свободно собирать, хранить и использовать информацию о своих пользователях, причем без всяких ограничений, зарабатывать на ней и ни с кем не делиться доходами от такого рода деятельности.

— Государство хочет иметь максимально полную информацию о своих гражданах, ограничивая в этом сборе бизнес [2].

В данной ситуации предвидится один самый рациональный выход – обеспечение правовой основы вовлечения субъекта персональных данных в оборот его данных; введение гражданина, как полноправного участником рынка ПД, заинтересованного в качестве и полноте его «цифрового профиля».

В настоящее время эта система не работает или же всё находится в зачаточном состоянии. Поэтому пользователь должен сам стремиться к защите своих персональных данных. Есть несколько способов сделать это:

— Каждая социальная сеть – это бесценный источник информации для злоумышленников, собирающих персональные данные. Поэтому важно правильно настроить конфиденциальность профиля. Как минимум нужно использовать двухфакторную аутентификацию.

— В нашей почте хранятся «ключи» от большинства наших учетных записей, так как процедура восстановления пароля чаще всего осуществляется именно с помощью email-сообщений. Поэтому жизненно необходимо обезопасить свой основной почтовый адрес. Для регистрации на сомнительных ресурсах необходим дополнительный адрес электронной почты.

— Недавно компания Google запустила специальный инструмент «О себе», позволяющий пользователям проверить, какие личные данные они опубликовали с помощью разных Google-сервисов. С его помощью можно узнать много интересного [3].

— Пока единственным способом ограничить себя от постоянной слежки в интернете, сохраняя при этом привычные социальные связи, является использование браузерных версий сервисов вместо соответствующих им приложений. В этом случае пользователь жертвует удобством, но значительно ограничивает для этих сервисов доступ к записной книжке, геолокации, списку установленных приложений и другим данным, хранящимся на вашем смартфоне. В отличие от мобильных приложений, веб-версии обычно продолжают работать, даже если не выдать им разрешение на доступ к GPS [4].

Очевидно, что злободневные для IT-сферы вопросы коммерциализации персональных данных и определения понятия bigdata остаются пока без однозначных ответов и еще требуют проработки: доктринальной, законодательной, правоприменительной. Исходя из мнений экспертов можно заключить лишь, что большинство все же придерживаются позиции о необходимости в первую очередь заботиться о защите прав субъектов персональных данных на охрану достоинства и частной жизни. Именно в таком русле сформировано сейчас и продолжает развиваться российское законодательство [5].

Наиболее прогрессивно сейчас с этим обстоят дела в Европе – там задали новые стандарты в части культуры сбора, хранения и использования данных. Требуется не только согласие пользователя, но и законная цель. В противном случае компанию ждут серьезные проблемы – штрафы, запрет на деятельность на европейском рынке. Крайне желательно перенять этот опыт.

Список литературы

[1]. Бевза Д. Что происходит с персональными данными и почему они нам не принадлежат. – 2019. – С. 1–10.

[2]. *О персональных данных* – Роскомнадзор. – URL: <https://77.rkn.gov.ru/p3852/p13239/p13309/> (дата обращения 30.10.2020)

[3]. *Как защитить личные данные в интернете.* – URL: <https://www.kaspersky.ru/blog/privacy-ten-tips/10390/> (дата обращения 1.11.2020)

[4]. *Как защитить персональные данные в интернете.* – URL: <https://data-sec.ru/personal-data/how-to-protect/> (дата обращения 1.11.2020)

[5]. *Коммерциализация персональных данных и понятие «биг дата» - злободневные вопросы IT-сферы.* – URL: <http://www.garant.ru/article/1229761/> (дата обращения 1.11.2020)

Малахов Павел Юрьевич – студент КФ МГТУ им. Баумана. E-mail: pavel.mologec@gmail.com

Лачихина Анастасия Борисовна – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anastisialach73@gmail.com

О ВАЖНОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РЕАЛИЯХ 2020 ГОДА

Вопрос безопасности персональных данных является актуальным на протяжении многих лет. Но 2020 год внес особенную остроту в данную сферу, благодаря пандемии. Находясь на самоизоляции, люди вынуждены были обращаться за услугами, работать и учиться дистанционно. Поспешный массовый переход на цифровые услуги неподготовленных слоев населения дал почву для взлета числа киберпреступлений. Связаны они в основном с хищением персональных данных пользователей, таких как номеров банковских карт, данных паспорта и других немаловажных документов.

Компании, предоставляющие услуги в сети Интернет, принимают меры по обеспечению информационной безопасности своих ресурсов. Но, как говорится, спасение утопающих – дело рук самих утопающих. Если люди не будут сами заботиться о своих персональных данных, как о личном имуществе, никто не сможет им помочь.

Основная проблема заключается в том, что многие не просто не знают, каким образом можно обезопасить свои персональные данные, но даже не задумываются, что это такое, и каким опасностям они подвергаются.

Так что такое защита персональных данных и что надо защищать?

Защита персональных данных – комплекс мероприятий организационно-технического характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Защита персональных данных включена в раздел охраны труда на предприятиях, является самостоятельным элементом. Государство гарантирует работникам защиту их персональных данных, а также их права на труд, с учетом использования их персональных данных (например, паспорт).

К персональным данным относятся:

1. фамилия, имя, отчество;
2. год, месяц, дата и место рождения;
3. адрес места регистрации и проживания;
4. семейное, социальное, имущественное положение;
5. образование, профессия, доходы;
6. паспортные данные;
7. отношение к религии;
8. национальность;
9. сведения, которые характеризуют физиологические и биологические особенности человека.

Номер телефона (цифры) не являются персональными данными. Номер телефона может являться персональными данными только в совокупности с ФИО.

Защита персональных данных гарантируется государством и регламентируется федеральным законом 153-ФЗ «О персональных данных» от 27.07.2006.

Но далеко не все зависит от усилий государства и операторов обработки персональных данных. Многие зависят от самих граждан. И здесь важную роль играет осознанность действий людей.

Для оповещения пользователей о проблемах, связанных с защитой персональных данных, было предложено несколько решений. Одним из них является проект, идея которого заключается в создании набора креативных просветительских плакатов, ориентированных в первую очередь на молодежь, и которые можно было бы распространять как в бумажном, так и в электронном виде. Такие плакаты можно развешивать на стенах коридоров в учебных заведениях. Во время перемен они привлекали бы к себе взгляды школьников и студентов, ненавязчиво предоставляя полезную информацию. Попадаясь на глаза изо дня в день, информация отпечатывается в голове. Школы, средние и высшие учебные заведения сейчас работают в очном и дистанционном формате. Учителя создают беседы в WhatsApp и Viber для родителей и учеников. Преподаватели общаются со студентами в VK или Телеграмме. Многие активно используют Instagram или YouTube для мастер-классов. Эти каналы распространения информации от педагогов к ученикам и родителям вполне можно было бы использовать для распространения просветительской информации о персональных данных. Кроме того, большинство учебных заведений имеют официальные сайты и группы во многих социальных сетях.

Еще одним решением проблемы защиты персональных данных является программный продукт, задачей которого является оповещение пользователей о том, что данный сайт будет запрашивать личные данные. Приложение работает в фоновом режиме, не мешая работе. При открытии сайта в браузере происходит проверка на наличие данного сайта в списке часто посещаемых сайтов, на которых запрашиваются персональные данные пользователя. Если происходит совпадение, то приложение выдает всплывающее предупреждение.

Список литературы

[1]. *Абаев Ф.А.* Понятие, правовая природа персональных данных // Право и государство: теория и практика. – 2014. – № 3 (111). – С. 126-131.

[2]. *Важорова М.А.* Соотношение понятий «информация о частной жизни» и «персональные данные» // Вестник Саратовской государственной юридической академии. – 2012. – № 4 (86). – С. 55-59.

Козин Сергей Владимирович – студент КФ МГТУ им. Н.Э. Баумана.
E-mail: k0zinsergey@yandex.ru

Каян Павел Дмитриевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: exorr3@mail.ru

Волков Александр Михайлович – студент КФ МГТУ им. Н.Э. Баумана.
E-mail: s79202725752@yandex.ru

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ KUBERNETES

Введение. Ритм развития информационных технологий в современном мире активно набирает обороты. Ежегодно создаются сотни технологий и выпускаются тысячи приложений, способных значительно упростить жизнь человека, усовершенствовать действующие системы, при этом обеспечив не только комфорт пользователей, но и стабильность работы и безопасность данных. Одной из таких технологий стал Kubernetes, который, не смотря на столь недавнее появление, на данный момент является одним из инновационных решений в компьютерной индустрии.

Устройство технологии Kubernetes. Kubernetes (K8s) – это система с открытым исходным кодом для автоматизации развертывания, масштабирования и управления контейнерными приложениями [1]. Корпорация Google в 2014 году занялась разработкой данной системы для внутренних нужд, основываясь на десятилетнем опыте работе с масштабными рабочими нагрузками, в сочетании с лучшими в своем классе идеями и практиками сообщества. Версия Kubernetes 1.0 была выпущена 21 июля 2015 года, после чего Google в партнерстве с Linux Foundation организовала специальный фонд Cloud Native Computing Foundation (CNCF), которому корпорация передала Kubernetes в качестве начального технологического вклада. Активное применение технологии K8s началось лишь в последние несколько лет. На текущий момент, Kubernetes используют такие крупные корпорации как Google, Adidas, Babylon, OpenAI, Booking.com, Spotify, VSCO, Wikimedia и многие другие.

В практике администрирования Kubernetes используется понятие подов (pods). Каждый под – это группа объединенных общей задачей контейнеров (к примеру, на том же Docker), которые могут быть и микросервисом, и массивным приложением, разнесенным на несколько параллельно работающих машин. K8s призван решать проблемы с эффективным распределением выполнения контейнеров по узлам кластера в зависимости от изменения нагрузки и текущей потребности в сервисах. Иными словами, Kubernetes – это система гибкого управления инфраструктурой контейнеризации с возможностью балансировки нагрузки, обеспечивающая скорость, гибкость технологии и экономическую эффективность [2].

По своей сути Kubernetes представляет собой один из стратегических компонентов всего DevOps-процесса, именно поэтому атаки на него всегда были и остаются актуальными. Взломав эту систему, хакер получит доступ ко всем узлам контейнерам, запущенным внутри K8s, а это уже прямой путь и к компрометации или утечке конфиденциальных данных. Именно поэтому необходимо обеспечить высокую степень кибербезопасности при использовании данной технологии.

Векторы атак наKubernetes. Kubernetes имеет довольно сложную архитектуру и использует в своем составе множество компонентов, поэтому векторы и типы атак на него тоже разнятся.

Основные из них:

— MasterNode – главный мастер-сервер, управляющий всем кластером рабочих узлов (подов) и развертыванием модулей на этих узлах;

— WorkerNode – рабочие серверы, на которых запускают контейнеры приложений и другие компоненты Kubernetes, к примеру такие, как K8s-агенты и прокси-серверы;

— Pods – это неделимая элементарная единица развертывания и адресации в Kubernetes. Под имеет собственный IP-адрес и может содержать один или несколько контейнеров;

— Services – сетевые службы, обеспечивающие обмен данными внутри кластера, балансировку, репликацию, обрабатывающие запросы и т.д.;

— SystemComponents – ключевые системные компоненты, которые используются для управления кластером Kubernetes: сервер API, Kubelet и другие [2].

Данные части системы являются ключевыми и наиболее подвержены хакерским атакам, а значит, требуют особого подхода к обеспечению кибербезопасности.

Проблемы безопасности Kubernetes. Хотя Kubernetes является достаточно сложной системой, но и в ней были найдены различные уязвимости, некоторые из которых можно отнести к критическим. Рассмотрим несколько из них:

1. Explosion of East-West Traffic («Взрыв трафика Восток–Запад») – атака, при которой контейнеры могут быть динамически развернуты в нескольких независимых друг от друга облаках, что значительно увеличивает трафик обмена данными внутри логического кластера. Удаленное расположение контейнеров может использоваться злоумышленниками, например, для реализации DDoS-атак.

2. Increased Attack Surface (увеличенная площадь атаки) – проблема безопасности, основывающаяся на том, что каждый контейнер может иметь различную поверхность атаки и собственные уникальные уязвимости, которые используются хакерами для дальнейшего взлома. К примеру, могут использоваться уязвимости для Docker или системы авторизации AWS.

3. Container compromise (компрометация контейнера) – проблема безопасности кроется в использовании неверной конфигурации (security misconfiguration) для всех контейнеров кластера, которые косвенным образом способствуют компрометации или же включают в себя уязвимости приложений. К компрометациям контейнера относятся манипуляции внутренней конфигурацией, управлением процессами или доступом к файловой системе.

4. Unauthorized connections between pods (несанкционированные соединения между подами внутри единого кластера). Скомпрометированные контейнеры могут соединяться с другими контейнерами на том же или на других

хостах, чтобы запустить какую-либо атаку. Несмотря на то, что фильтрация на уровне L3 (ACL-листы) обеспечивается сетевым оборудованием согласно настроенным правилам, некоторые неавторизованные обращения могут быть обнаружены только с помощью фильтрации на седьмом уровне модели OSI [2].

Данные атаки являются наиболее распространенными и требуют особого внимания со стороны разработчиков и системных администраторов.

Ежегодно в системе Kubernetes обнаруживаются новые уязвимости, однако данная технология продолжает развиваться, становится всё более распространенной в мировых компаниях и ведет активную работу по обеспечению безопасности данных. В течение 4-х лет (2016-2019 гг.) были найдены и исправлены 17 критических уязвимостей [2]. Но ввиду специфики устройства технологии, обеспечить максимальную безопасность данных только на уровне самого Kubernetes невозможно – важно использовать методы обеспечения безопасности на пользовательском уровне.

Методы обеспечения кибербезопасности при использовании Kubernetes. K8s имеет внутренние способы защиты данных, среди которых важно выделить KubernetesSecret.

Secret – это объект, который может быть использован в K8s для хранения конфиденциальных данных. Размещение конфиденциальной информации в секретном объекте не делает его автоматически безопасным. По умолчанию данные в секретах Kubernetes хранятся в кодировке Base64, которая практически не отличается от обычного текста [3].

Однако секреты дают вам больше контроля над доступом и использованием паролей, ключей и т.д. Kubernetes может монтировать секреты отдельно от модулей, которые их используют, или сохранять их как переменные среды.

Встроенный механизм секретов в Kubernetes обеспечивает базовые возможности безопасности, такие как включение шифрования в состоянии покоя, определение политик авторизации и белый список доступа к конкретным экземплярам контейнера.

Однако эти основные меры безопасности не применяются по умолчанию, и даже если они включены, их недостаточно для большинства организаций. Для обеспечения безопасности приложений, развернутых в Kubernetes, важно обратить внимание на следующие рекомендации:

— Отслеживание конфигураций по умолчанию: все конфигурации Kubernetes по умолчанию должны необходимо проверять перед использованием, чтобы минимизировать риск того, что атака внутри одного модуля может распространиться на другие модули.

— Контроль среды выполнения контейнера: Kubernetes не имеет защиты от атак во время выполнения и не может обнаруживать вторжения после их возникновения, поэтому в случае, если в работающем контейнере обнаружена активная брешь или новая уязвимость, необходимо уничтожить весь контейнер и перезапустить некомпрометированную версию.

— Сканирование образов (images): плохо настроенные образы контейнеров предоставляют злоумышленникам легкую точку доступа для проникновения в сеть, а образы, содержащие определенные ключи аутентификации, могут помочь киберпреступникам в дальнейших атаках. Для обнаружения вредоносного кода внутри образа контейнера, требуется сканирование уязвимостей в реестрах и в производственной среде с помощью сторонних приложений.

— Обеспечение безопасности хоста: Kubernetes запускает контейнеры на назначенных ему серверах, не гарантирующих кибербезопасность. Можно обратиться к традиционным средствам безопасности для обнаружения эксплоитов в отношении системных ресурсов, но если хост также будет скомпрометирован, это может привести к разрушительным последствиям. Хост-системы необходимо отслеживать на предмет взломов и подозрительных действий для отражения злонамеренных атак с помощью необходимого ПО.

— Контроль связи между капсулами: по умолчанию Kubernetes не применяет сетевую политику к каждому модулю, поскольку это «подрывает» безопасность: хакерам потребуются взломать лишь один контейнер, чтобы затем переместиться в боковом направлении внутри среды. Связывание сетевой политики с модулем является аналогичным правилам брандмауэра и контролирует, что модуль может взаимодействовать только с определенными активами [4].

В настоящее время существует множество инструментов, способных помочь отследить и устранить уязвимости для обеспечения безопасности Kubernetes. Они помогают сканировать образы Kubernetes и проводить статический анализ, обеспечивать runtime-безопасность, сетевую и комплексную безопасность Kubernetes, распространять образы и управлять секретами, проводить аудит безопасности системы [5]. Среди них Anchore, Clair, Aporoto, Portieris, Kubeaudit, Aqua Security, Sysdig и другие.

Помимо всего этого на официальном сайте Kubernetes можно найти рекомендации по обеспечению кибербезопасности в зависимости от требуемой специфики кластера.

Заключение. В настоящее время всё больше компаний по всему миру внедряют в свои системы технологию Kubernetes ввиду её гибкости, скорости и экономической эффективности, но это требует от них особого контроля безопасности. В настоящее время существует достаточно много методов для обеспечения кибербезопасности данных и приложений при использовании технологии K8s. Обеспечение безопасности контейнеров Kubernetes имеет решающее значение для защиты сетей и приложений от взломов и злонамеренных атак, именно поэтому важно успешно интегрировать безопасность на каждом этапе жизненного цикла контейнера Kubernetes.

Список литературы

[1] *Что такое Kubernetes?* – URL: <https://kubernetes.io/ru/docs/concepts/overview/what-is-kubernetes/> (дата обращения 27.10.2020).

[2] *Пискунов И.* Непробиваемый DevOps-кластер. Настраиваем и усиливаем безопасность Kubernetes. – URL: <https://hakер.ru/2019/08/28/bulletproof-kubernetes/#toc02.1> (дата обращения 29.10.2020)

[3] *What is Kubernetes Container Security?* – URL: https://www.trendmicro.com/en_ca/what-is/container-security/kubernetes.html (дата обращения 28.10.2020).

[4] *Rani Osnat.* Protecting Kubernetes Secrets: A Practical Guide. – URL: <https://blog.aquasec.com/managing-kubernetes-secrets> (дата обращения 30.10.2020).

[5] *Mateo Burilo.* 33(+) K8s Security Tools. – URL: <https://sysdig.com/blog/33-kubernetes-security-tools/> (дата обращения 30.10.2020)

Липатова Софья Евгеньевна – студент КФ МГТУ им. Н.Э. Баумана.
E-mail: sonya_lipatova@list.ru

Гагарин Юрий Евгеньевич – канд. техн. наук, заведующий кафедрой «Программное обеспечение ЭВМ, информационные технологии» КФ МГТУ им. Н.Э. Баумана. E-mail: Yriigagarin@yandex.ru

ОБЗОР АЛГОРИТМОВ РАСПОЗНАВАНИЯ ЛИЦ, ПРИМЕНЯЕМЫХ ДЛЯ АУТЕНТИФИКАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

На сегодняшний день парольные алгоритмы аутентификации в различных автоматизированных системах является де-факто минимально обязательным и необходимым механизмом для обеспечения информационной безопасности этих систем. Однако для усиления безопасности и защиты в таких системах может применяться многоуровневая аутентификация в дополнение к парольным алгоритмам защиты. Одним из таких уровней может быть биометрическая аутентификация с использованием алгоритмов распознавания лиц.

Исторически первыми были разработаны и применены на практике геометрические алгоритмы. Их применение было связано с простотой вычислений для данных алгоритмов. При распознавании лиц данным способом выделяются ключевые точки с использованием детекторов глаза, рта и носа, анализируется их взаимное расположение. Более эффективным развитием данных алгоритмов являются алгоритмы распознавания на основе карты краевых линий. Суть алгоритма состоит в выделении в исходном изображении краев с разными пороговыми значениями, и сравнение полученного набора с картой краев модели посредством вычисления расстояния по Хаусдорфу.

Основная проблема при разработке систем распознавания на основе данного вида алгоритмов – выбор множества характерных точек, однозначно описывающих конкретное человеческое лицо. Реализация данных алгоритмов невозможна без учета следующих требований: точки на лице или черты лица, на которых основывается идентификация, не должны закрываться прической, бородой, маской и другими посторонними предметами; для обеспечения независимости процесса распознавания от масштаба изображения целесообразно описывать систему идентификационных точек в отношениях между ними; выбранная система точек должна обеспечивать относительную устойчивость процесса распознавания при незначительном изменении ракурса съемки (легкий поворот головы, наклон, изменение выражения лица и т.д.); количество характерных точек системы, удовлетворяющей вышеизложенным требованиям, должно быть минимальным, так как вычислительная стоимость алгоритмов обычно пропорциональна их количеству.

Алгоритм собственных векторов (иногда его называют алгоритм главных компонент лиц) является более проработанным по сравнению с геометрическими алгоритмами.

Он является примером того, как математические алгоритмы (алгоритм анализа главных компонент), успешно применявшиеся в других областях, оказались эффективно адаптированными к распознаванию людей по их лицам.

Суть алгоритма заключается в следующем – любое цифровое изображение представляется в виде вектора в пространстве лицевых признаков. Если

изображение описывается $x \times y$ пикселями, размерность простейшего векторного пространства, к которому данный вектор принадлежит, будет равна произведению x на y и, соответственно, базис подобного векторного пространства будет состоять из $x \times y$ векторов. Однако из-за схожести человеческих лиц между собой (овальная форма с носом, ртом, глазами и т.д.), все векторы, описывающие изображения лиц, будут размещаться в узко ограниченной области данного векторного пространства. Поэтому при решении задачи распознавания людей по лицу описание и хранение всего векторного пространства не рационально. Исходя из этого, встает вопрос построения пространства с компактным по размерам векторам. Возможным является пространство, базисными векторами которого служат главные компоненты всех содержащихся в нем изображений лиц. Размерность такого пространства заранее определить невозможно, но оно намного меньше размерности векторного пространства всех изображений. Из вышесказанного вытекает, что главной целью алгоритма анализа принципиальных компонент является значительное уменьшение размерности пространства признаков таким образом, чтобы оно как можно лучше описывало типичные образы, принадлежащие множеству лиц. При применении данного алгоритма для идентификации лиц используются обучающие наборы изображений, по которым строятся переменные изменчивости. Эти переменные представляют собой $x \times y$ - размерные векторы, которые называются собственными. Если преобразовать подобные векторы в изображения, то получаемые картинки будут отражать главные компоненты представленного обучающего множества (также называемые собственными лицами). В итоге, за счет снижения размерности пространства базисных векторов, в котором находятся изображения, добиваются хороших показателей как в скорости, так и в точности распознавания лиц.

Аналогично предыдущему алгоритму на базе обучающих изображений возможно применение двух других типов алгоритмов – использования вероятностного подхода при сравнении и использование нейронных сетей.

Использование вероятностного подхода подразумевает формирование двух классов разделения для лиц: 1) портрет данного человека, 2) все другие портреты. Функции плотности вероятности для каждого класса оцениваются при помощи обучающего множества и впоследствии используются для вычисления степени схожести, которая основывается на полученных опытным путем вероятностных характеристиках. В дополнение для получения более точных результатов может использоваться вероятностная модель некоторого физического процесса, по которой и формируется окончательная мера схожести двух изображений.

При использовании нейронных сетей для совокупности входных объектов необходимо сформировать такую же совокупность на основе данных сети и сопоставить результаты. Входным объектом для данной сети служит изображение лица человека. Нейрон в сети – это простейшая ячейка памяти. Последовательность работы нейронных сетей следующий: сначала изображение оцифровывается и кодируется в набор векторов; потом каждая координата век-

тора располагается в отдельной ячейке, связанной совсеми остальными ячейками (обучение или настройка системы происходит путем изменения весов связей между ячейками); наконец изображения лиц фильтруются через нейросеть, при этом входное изображение трансформируется в ближайшее сохраненное подается на сравнение.

Подытожив все вышеперечисленное, можно сказать, для разработчиков систем и подсистем аутентификации существуют различные классы алгоритмов, которые могут быть использованы исходя из поставленных задач и имеющихся ресурсов. Однако использование любого из вышеперечисленных алгоритмов позволяет повысить уровень безопасности практически любой автоматизированной системы.

Список литературы

[1] Самаль Д.И., Старовойтов В.В. Обзор Существующих Подходов И Методов Распознавания людей по фотопортретам. – URL: https://www.researchgate.net/publication/236605649_OBZOR_SUSESTVUUSIH_PODHODOV_I_METODOV_RASPOZNAVANIA_LUDEJ_PO_FOTOPORTRE TAM (дата обращения 29.10.2020)

[2] Бун К.Л. Face Detection: A Survey. – URL: <https://www.semanticscholar.org/paper/Face-Detection%3A-A-Survey-Hjelm%С3%A5s-Low/887567782cb859ecd339693589056903b0071353>

[3] Старовойтов В.В., Брилюк Д.В. Распознавание человека по изображению лица нейросетевыми методами, – URL: http://uiip.bas-net.by/structure/1_ori/starovoitov/Starovoitov_Publication_section/11_Starovoitov02_prep.pdf (дата обращения 29.10.2020)

[4] PCI SECURITY STANDARDS. – URL: https://www.pcisecuritystandards.org/documents/PCI-Secure-Software-Standard-v1_0.pdf (дата обращения 29.10.2020)

Филатов Александр Романович – студент КФ МГТУ им. Н.Э. Баумана.
E-mail: afnotdead@yandex.ru

ОБЗОР СУЩЕСТВУЮЩИХ АЛГОРИТМОВ РАСПОЗНАВАНИЯ ЛИЦ

Существует большое разнообразие алгоритмов распознавания лиц, но у всех лежит в основе следующая последовательность процессов:

1. Детектирование лица.
2. Геометрическое и яркостное выравнивание лица.
3. Определение специфических признаков.
4. Сравнение признаков с эталонными.

Основным отличием всех алгоритмов является вычисление признаков и сравнение их совокупностей между собой.

Метод гибкого сравнения на графах (Elastic graph matching). Данный метод основан на сопоставлении графов, описывающих изображения лиц. Лица представляются в виде графов со взвешенными вершинами и ребрами. Во время распознавания эталонный граф остается неизменным, а второй изменяется с целью наилучшего сопоставления с первым. В вершинах графа вычисляются значения признаков, в большинстве случаев используются комплексные значения фильтров Габора или их упорядоченных наборов – Габоровских вейвлет (строи Габора), которые вычисляются в некоторой локальной области вершины графа локально путем свертки значений яркости пикселей с фильтрами Габора. Ребра графа взвешиваются расстояниями между смежными вершинами. Различие (расстояние, дискриминационная характеристика) между двумя графами вычисляется при помощи некоторой ценовой функции деформации, учитывающей как различие между значениями признаков, вычисленными в вершинах, так и степень деформации ребер графа.

Деформация графа происходит путем смещения каждой из его вершин на некоторое расстояние в определённых направлениях относительно ее исходного местоположения и выбора такой ее позиции, при которой разница между значениями признаков (откликов фильтров Габора) в вершине деформируемого графа и соответствующей ей вершине эталонного графа будет минимальной. Данная операция выполняется поочередно для всех вершин графа до тех пор, пока не будет достигнуто наименьшее суммарное различие между признаками деформируемого и эталонного графов. Значение ценовой функции деформации при таком положении деформируемого графа и будет являться мерой различия между входным изображением лица и эталонным графом. Данная «релаксационная» процедура деформации должна выполняться для всех эталонных лиц, заложенных в базу данных системы. Результат распознавания системы – эталон с наилучшим значением ценовой функции деформации. Недостатки: высокая вычислительная сложность процедуры распознавания. Низкая технологичность при запоминании новых эталонов. Линейная зависимость времени работы от размера базы данных лиц [1].

Нейронные сети. В настоящее время существует около десятка разновидностей нейронных сетей (НС). Одним из самых широко используемых вариантов является сеть, построенная на многослойном перцептроне, которая позволяет классифицировать поданное на вход изображение/сигнал в соответствии с предварительной настройкой сети.

Обучаются нейронные сети на наборе готовых примеров. Суть процесса сводится к настройке весов межнейронных связей в процессе решения оптимизационной задачи методом градиентного спуска. В процессе обучения НС происходит автоматическое извлечение ключевых признаков, определение их важности и построение взаимосвязей между ними. Предполагается, что нейронная сеть сможет применить опыт, полученный в процессе обучения, на неизвестные образы за счет обобщающих способностей.

Наилучшие результаты в области распознавания лиц (по результатам анализа публикаций) показала Convolutional Neural Network или сверточная нейронная сеть (далее – СНС), которая является логическим развитием идей таких архитектур НС как когнитрона и неокогнитрона. Успех обусловлен возможностью учета двумерной топологии изображения, в отличие от многослойного перцептрона.

Отличительными особенностями СНС являются локальные рецепторные поля (обеспечивают локальную двумерную связность нейронов), общие веса (обеспечивают детектирование некоторых черт в любом месте изображения) и иерархическая организация с пространственным сэмпингом (spatial subsampling). Благодаря этим нововведениям СНС обеспечивает частичную устойчивость к изменениям масштаба, смещениям, поворотам, смене ракурса и прочим искажениям. Недостатком нейронных сетей является то, что добавление нового эталонного лица в базу данных требует полного переобучения сети на всем имеющемся наборе (достаточно длительная процедура, в зависимости от размера выборки от 1 часа до нескольких дней) [2].

Скрытые Марковские модели (СММ, НММ). Одним из статистических методов распознавания лиц являются скрытые Марковские модели (СММ) с дискретным временем. СММ используют статистические свойства сигналов и учитывают непосредственно их пространственные характеристики. Элементами модели являются: множество скрытых состояний, множество наблюдаемых состояний, матрица переходных вероятностей, начальная вероятность состояний. Каждому соответствует своя Марковская модель. При распознавании объекта проверяются сгенерированные для заданной базы объектов Марковские модели и ищется максимальная из наблюдаемых вероятностей того, что последовательность наблюдений для данного объекта сгенерирована соответствующей моделью.

На сегодняшний день СММ в коммерческих целях не используется.

Недостатки:

– необходимо подбирать параметры модели для каждой базы данных;

– СММ не обладает различающей способностью, то есть алгоритм обучения только максимизирует отклик каждого изображения на свою модель, но не минимизирует отклик на другие модели.

Active Appearance Models (AAM). Активные модели внешнего вида (Active Appearance Models, AAM) – это статистические модели изображений, которые путем разного рода деформаций могут быть подогнаны под реальное изображение. Данный тип моделей в двумерном варианте был предложен Тимом Кутсом и Крисом Тейлором в 1998 году. Первоначально активные модели внешнего вида применялись для оценки параметров изображений лиц.

Активная модель внешнего вида содержит два типа параметров: параметры, связанные с формой (параметры формы), и параметры, связанные со статистической моделью пикселей изображения или текстурой (параметры внешнего вида). Перед использованием модель должна быть обучена на множестве заранее размеченных изображений. Разметка изображений производится вручную. Каждая метка имеет свой номер и определяет характерную точку, которую должна будет находить модель во время адаптации к новому изображению. Процедура обучения ААМ начинается с нормализации форм на размеченных изображениях с целью компенсации различий в масштабе, наклоне и смещении. Для этого используется так называемый обобщенный Прокрустов анализ. Из всего множества нормированных точек затем выделяются главные компоненты с использованием метода РСА. Далее из пикселей внутри треугольников, образуемых точками формы, формируется матрица, такая что, каждый ее столбец содержит значения пикселей соответствующей текстуры. Стоит отметить, что используемые для обучения текстуры могут быть как одноканальными (градации серого), так и многоканальными (например, пространство цветов RGB или другое). В случае многоканальных текстур векторы пикселей формируются отдельно по каждому из каналов, а потом выполняется их конкатенация. После нахождения главных компонент матрицы текстур модель ААМ считается обученной [3].

Active Shape Models (ASM). Суть метода ASM заключается в учете статистических связей между расположением антропометрических точек. На имеющейся выборке изображений лиц, снятых в анфас. На изображении эксперт размечает расположение антропометрических точек. На каждом изображении точки пронумерованы в одинаковом порядке. Для того чтобы привести координаты на всех изображениях к единой системе обычно выполняется т.н. обобщенный прокрустов анализ, в результате которого все точки приводятся к одному масштабу и центрируются. Далее для всего набора образов вычисляется средняя форма и матрица ковариации. На основе матрицы ковариации вычисляются собственные вектора, которые затем сортируются в порядке убывания соответствующих им собственных значений. Однако все же главной целью ААМ и АСМ является не распознавание лиц, а точная локализация лица и антропометрических точек на изображении для дальнейшей обработки.

В заключение следует отметить, что несмотря на всё разнообразие алгоритмов, при проведении глобальных тестирований (например, программа FERET, разработанная агентством DARPA и исследовательской лабораторией армии США) эффективность всех алгоритмов оказалась примерно одинаковой. Из-за этого трудно или даже невозможно провести четкие различия между ними и выделить лучший. Основными критериями для выбора алгоритма стали доступность библиотек и примеров и сложность алгоритма. Поэтому для реализации был выбран метод гибкого сравнения на графах.

Список литературы

[1]. *Попов Д.И., Воробьев Е.В.* Компьютерная графика. – М.: Издательство МГУП, 2014. – 70 с.

[2]. <https://habr.com/ru/company/synesis/blog/238129/> (дата обращения 28.10.2020)

[3].
https://www.researchgate.net/publication/221305430_Face_Recognition_Using_Active_Appearance_Models (дата обращения 28.10.2020)

Рунов Илья Евгеньевич – студент КФ МГТУ им. Н.Э. Баумана.
E-mail: ierunov@yandex.ru

ОБОСНОВАНИЕ ВЫБОРА НЕКОНТРОЛИРУЕМЫХ АЛГОРИТМОВ С ПОМОЩЬЮ АТАК И КЛАССОВ АНОМАЛИЙ

Введение. Обнаружение аномалий направлено на поиск закономерностей в данных, которые не соответствуют ожидаемому поведению. Он в значительной степени используется в системах обнаружения вторжений, полагаясь на неконтролируемые алгоритмы, которые потенциально могут обнаруживать атаки нулевого дня; однако эффективность алгоритмов варьируется в зависимости от наблюдаемой системы и атак. Выбор алгоритма, который максимизирует возможности обнаружения, является сложной задачей без мастер-ключа.

Современные системы, такие как киберфизические инфраструктуры, системы систем или облачные среды, могут быть нацелены на кибератаки, требующие внимательных контрмер безопасности. Детекторы вторжений (IDs) были предложены для повышения безопасности путем анализа системных данных, направленных на выявление подверженных ошибкам, вредоносных или несанкционированных действий. IDs могут применять методы, основанные на сигнатурах, которые состоят из проверки свойств или поиска паттернов (сигнатур) в контролируемых данных для обнаружения проявления неисправности или продолжающейся атаки [4].

Сигнатурные подходы обладают хорошими возможностями обнаружения при работе с известными неисправностями или атаками, но они могут потерпеть неудачу при идентификации неизвестных неисправностей [2]. Кроме того, когда обнаруживается неизвестная ошибка или атака нулевого дня, (то есть атака, использующая новые или неоткрытые уязвимости системы), новая сигнатура должна быть быстро разработана и добавлена к набору сигнатур.

Чтобы иметь дело с неизвестными, исследователи перешли к методам, пригодным для обнаружения невидимых, новых атак. Детекторы аномалий основаны на предположении, что атака генерирует наблюдаемые отклонения от ожидаемого поведения, и они направлены на поиск паттернов в данных, которые не соответствуют ожидаемому поведению системы: такие паттерны известны как аномалии. В данной работе будет сделан упор на неконтролируемых алгоритмах обнаружения аномалий, которые подходят для обнаружения, в частности, атак нулевого дня, без необходимости использования меток в обучающих данных [3].

Семейства неконтролируемых алгоритмов. Будет рассмотрено шесть семейств неконтролируемых алгоритмов, обычно используемых в литературе, анализируя их основные характеристики. Также, стоит отметить, что между семьями существуют некоторые неизбежные семантические совпадения:

– Алгоритмы кластеризации разбивают набор точек данных таким образом, чтобы точки данных в одной и той же группе (кластере) имели

сходные характеристики. Точки данных, которые не могут быть отнесены ни к одному из существующих кластеров или которые не удовлетворяют определенным критериям включения, являются аномальными;

– Алгоритмы на основе соседей учатся по аналогии: они помечают точку данных как аномальную или ожидаемую в зависимости от метки её ближайшего соседа (соседей), рассматривая f -мерное пространство. В бесконтрольном режиме они используют расстояние точки данных от её соседей в качестве оценки аномалий;

– Алгоритмы на основе углов связывают данные с многомерными пространствами и измеряют дисперсию углов между точкой данных и другими точками. Ожидаемые точки данных имеют большую дисперсию угла, в то время как аномалии обычно приводят к очень малой дисперсии тройных точек;

– Алгоритмы классификации идентифицируют новую точку данных класса a в зависимости от информации, собранной во время предыдущих действий, например, отнесения данного сообщения электронной почты к классам спама или неспама. Несмотря на то, что они были рождены для контролируемых установок, они могут работать без присмотра;

– Алгоритмы на основе плотности оценивают плотность окрестности каждой точки данных. Когда точка данных отличается от ожиданий, она находится в области с низкой плотностью и затем помечается как аномальная;

– Статистические алгоритмы предполагают, что ожидаемые точки данных возникают в областях с высокой вероятностью данного статистического распределения. Они подгоняют распределение к ожидаемым точкам, а затем применяют статистический вывод, чтобы определить, принадлежит ли новая точка данных к этому распределению или нет. В бесконтрольном режиме статистические алгоритмы выводят базовое распределение по мере вычисления данных.

Исследование характеристик алгоритмов. Каждый алгоритм обнаружения неконтролируемых аномалий опирается на свои собственные свойства. По своим характеристикам, такие алгоритмы, как алгоритмы на основе соседей и алгоритмы на основе углов предназначены в основном для выявления точки аномалии, хотя они не могут быть в состоянии обнаружить коллективных аномалии, если размер выборки района меньше, чем размер коллектива группы аномалий [1]. Эта проблема разделяется также с некоторыми реализациями алгоритма *K-mean* (алгоритм кластеризации), так как коллективная аномалия может привести их к созданию отдельного кластера для конкретной группы точек данных. Алгоритмы классификации для обнаружения неконтролируемых аномалий часто идентифицируются как «СВМодного класса». Стоит отметить, что алгоритмы, выбранные для этого исследования, предназначены для представления внутренних характеристик различных семейств, а не самых последних вариантов существующих алгоритмов.

Заключение. Таким образом, результаты показывают, какие неконтролируемые алгоритмы более пригодны, чем другие, для обнаружения аномалий, принадлежащих к определенным классам(например, точечные аномалии будет легче всего обнаружить).

Вместо этого, за исключением углового алгоритма на основе соседей, легче всего обнаружить коллективные аномалии, чем контекстуальные и точечные аномалии. Этот результат объясняется следующим образом: выбранные алгоритмы используют большие обучающие наборы, которые позволяют тщательно и точно определить границы между аномальным и ожидаемым поведением. Однако в процессе обучения они выводят глобальную границу, которая не всегда подходит для обнаружения единичных аномалий, в то время как группы аномальных точек данных становятся легче идентифицировать.

Список литературы

[1] *Аверина Т.А.* Численные методы. Верификация алгоритмов решения систем со случайной структурой : учебное пособие для вузов / Т.А. Аверина. – М.: Издательство Юрайт, 2020.

[2] *Миркин Б.Г.* Введение в анализ данных : учебник и практикум / Б.Г. Миркин. – М.: Издательство Юрайт, 2020. – 174 с.

[3] *Папков Б.В.* Теория систем и системный анализ: учебник и практикум для вузов / Б.В. Папков, А.Л. Куликов. – 2-е изд., испр. и доп. – М.: Издательство Юрайт, 2020. – 470 с.

[4] *Черняк А.А.* Методы оптимизации: теория и алгоритмы : учебное пособие для вузов / А.А. Черняк, Ж.А. Черняк, Ю.М. Метельский, С.А. Богданович. – 2-е изд., испр. и доп. – М.: Издательство Юрайт, 2020. – 357 с.

Бандурина Екатерина Михайловна – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: bandurinakatya7@yandex.ru

Ерохин Илья Игоревич – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: drleiter@rambler.ru

М.Г. Шеленкова

ОБРАТИМОЕ СКРЫТИЕ ДАННЫХ ДЛЯ ДВОИЧНЫХ ИЗОБРАЖЕНИЙ

Главной задачей обеспечения безопасности информации является создание условий для поддержания её свойств – конфиденциальности, доступности и целостности.

Конфиденциальность гарантирует, что доступ к информации имеет узкий круг лиц, для кого она и предназначена. Обеспечивать конфиденциальность можно на различных этапах обработки и передачи информации, используя широкий спектр методов и средств.

Одним из подходов обеспечения конфиденциальности передаваемой информации является стеганография. Суть этого метода заключается в сокрытии самого факта передачи данных. В то время как шифрование приводит информацию к виду, при котором её нельзя понять, не зная алгоритма и ключа шифрования, стеганография скрывает информацию таким образом, чтобы её наличие и передача были неочевидными.

Перед началом процесса сокрытия информации стенографическая система должна идентифицировать избыточные биты – те биты, которые можно изменять без изменения целостности содержимого файла. После этого шага наименее значимые биты могут быть заменены данными, которые необходимо скрыть.

Бинарные изображения. Бинарное изображение – разновидность цифровых растровых изображений, когда каждый пиксель может представлять только один из двух цветов. Примерами бинарных изображений, в которые может быть встроена скрытая информация являются отсканированные и хранящиеся в формате изображений документы, QR-коды, штрих коды и т.п.

Из-за малой избыточности бинарных изображений (каждый пиксель может содержать только 0 или 1), встраивать данные в такие изображения становится затруднительно. Обычные методы сокрытия данных используют избыточность между пикселями изображения для встраивания данных.

В зависимости от того, можно ли восстановить исходные файлы или нет, методы подразделяются на сокрытие данных с потерями и сокрытие данных без потерь (также известное как обратимое сокрытие данных) соответственно [1].

Метод замены паттернов. Предположим, что двоичное изображение обозначено буквой B . Метод замены паттернов сначала преобразует изображение в матрицу разности по формуле 1. Матрица разности обозначена как D .

$$D = \left\{ \begin{array}{l} B(i, j), i = 1, j = 1 \\ B(i, j) \oplus B(i - 1, j), i \neq 1, j = 1 \\ B(i, j) \oplus B(i, j - 1) \end{array} \right\}, \square \quad (1)$$

где \oplus – «исключающее ИЛИ», i и j – позиция строки и столбца матрицы изображения соответственно [1].

Элемент в верхнем левом углу матрицы разницы содержит то же значение, что и исходное изображение, а остальные элементы со значением 1 матрицы разницы указывают на изменения в матрице изображения. То есть, для конкретного пикселя его значение в матрице разности D равно 1 тогда, когда значение пикселя отличается от предыдущего значения в матрице изображения. В противном случае его значение разности равно 0.

Предположим, что двоичный бит 0 используется для представления белого цвета, а бит 1 – для представления черного.

Пример изображения и его матрица разности показаны на рис. 1.

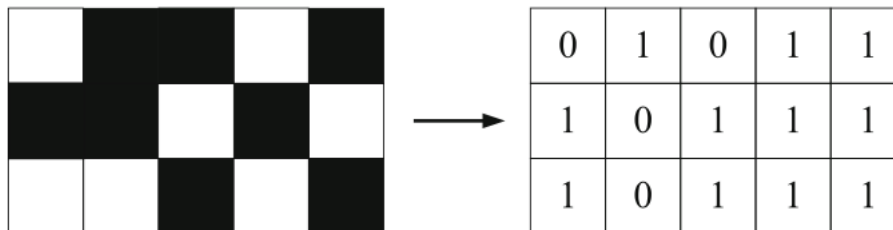


Рис. 1. Бинарное изображение и его матрица разности

В области матрицы разности четыре непрерывных бита образуют один паттерн. Следовательно, существует шестнадцать паттернов от D0000 до D1111. Эти паттерны обозначаются как от P0 до P15 или от P0000 до P1111.

Сначала метод замены паттернов преобразует изображение в область матрицы разности по формуле 1, а затем перед внедрением выбираются два конкретных паттерна для формирования пары паттернов. Затем кодировщик сканирует другую матрицу. Когда кодировщик встречает паттерн из этой пары, он встраивает один бит данных, используя механизм замены паттерна. После того, как все секретные биты встроены, встроеное изображение генерируется из модифицированной матрицы разности с помощью обратного уравнения 1.

Пара паттернов выбирается следующим образом. Предполагая, что дан один паттерн P_x , подходящий паттерн P_y для замены должен удовлетворять двум условиям, указанным ниже.

Условие 1. Когда происходит одна замена P_y на P_x в матрице разности, только один пиксель меняет свое значение в матрице изображения.

Условие 1 гарантирует минимальные искажения исходного изображения, изменяя один бит.

Условие 2: Все шестнадцать паттернов разделены на две группы. Образец с четным числом единиц относится к четной группе, а образец с нечетным числом единиц принадлежит к нечетной группе. P_y следует выбирать из той же группы P_x .

Например, шаблоны P0011 и P0010 принадлежат к разным группам, то есть P0011 принадлежит четной группе, а P0010 принадлежит к нечетной группе. Заменяем P0011 на P0010. Рассмотрим двоичную битовую последовательность B0010000 из изображения с предыдущим битом 0. Последовательность равна P0011000 после применения формулы (1).

Если её первый паттерн, то есть P0011, заменен паттерном P0010, измененная последовательность разницы будет P0010000. Встроенное изображение будет содержать последовательность V0011111 с помощью уравнения, обратного (1).

Видно, что между встроенной последовательностью бит V0011111 и исходной V0010000 битовая строка, следующая за первыми четырьмя битами, является инверсными друг относительно друга.

Следовательно, это вызовет довольно серьезные искажения исходного изображения. Однако если использовать два паттерна из одной группы четности, такого искажения не происходит.

Условие 1 гарантирует, что встраивание приводит к замене только одного пикселя внутри области паттерна в изображении, а условие 2 гарантирует, что пиксели вне области паттерна в изображении остаются такими же, когда происходит замена.

P0 представляет собой область с четырьмя белыми или черными пикселями на изображении. В этом типе паттерна даже переворот одного пикселя может вызвать серьезное искажение для человеческого зрения. Таким образом, P0 не используется в методе замены паттернов.

Количество всех пятнадцати паттернов подсчитывается путем растрового сканирования матрицы разницы слева направо и сверху вниз. Наиболее частый паттерн обозначен как PM, а наименее вероятный паттерн среди трех для него возможных обозначается как PF. Эти два шаблона выбираются для встраивания данных.

Механизм внедрения перестановки паттернов прост. Кодировщик сканирует матрицу разницы. Когда кодируемым паттерном является PM или PF, кодировщик встраивает секретный бит 0 путем перезаписи в PM и встраивает бит 1 путем перезаписи в PF.

Для восстановления изображения в процессе декодирования, положение PF записывается в карту местоположения, обозначенной LM, и оно должно быть записано после того, как будут внедрены все секретные данные.

Значения PM и PF должны быть записаны в качестве дополнительной информации и отправлены в декодер перед декодированием через защищенный канал. Декодер сканирует матрицу разности в том же порядке, что и кодировщик. Когда текущим паттерном является PM, декодер извлекает бит 0, или извлекает 1 в случае, когда паттерном является PF. Извлеченные данные включают две части: секретные данные и LM. Благодаря LM кодировщик может восстановить изображение.

В изображение встроены секретные данные, обозначенные как SD, равные 0110. Согласно последовательности PM и PF, значение LM равняется 00000100.

Предположим, что после сжатия без потерь сжатый LM, обозначенный как LMC, равен 0010, тогда общая последовательность данных для внедрения будет 01100010, что представляет собой SD с добавлением LMC. Затем мы заменяем паттерны PM и PF для встраивания данных. После того, как все дан-

ные встроены, уравнение обратное 1 используется для получения встроенного изображения.

В процессе извлечения данных встроенное изображение создает матрицу разности по формуле 1. В соответствии с последовательностью PM и PF в матрице разностей извлекаются SD и LMC. LMC распаковывается для получения LM. С помощью LM мы можем восстановить встроенную матрицу разности. Наконец, с помощью восстановленной матрицы можно получить исходное изображение по уравнению, обратному 1.

Вывод. В статье представлен метод сокрытия данных в бинарных изображениях, учитывающий малую избыточность исходных файлов и обеспечивающий обратимость процесса встраивания данных.

Список литературы

[1]. *Dong, Keming&Kim, Hyoung&Yu, Xiaohan&Feng, Xiaoqing.* Reversible data hiding for binary images based on adaptive overlapping pattern. EURASIP Journal on Information Security. 2020

[2]. *Y. A. Ho, Y. K. Chan, H. C. Wu, Y. P. Chu,* High-capacity reversible data hiding in binary images using pattern substitution. Comput. Stand. Interfaces. 31, 787–794 (2009)

Шеленкова Мария Геннадиевна – студент КФ МГТУ им. Н.Э. Баумана.
E-mail: marishelenok@gmail.com

ОПРЕДЕЛЕНИЕ ТИПОВ ФИШИНГОВЫХ АТАК И МЕТОДЫ ИХ ПРЕДОТВРАЩЕНИЯ

Введение. Сейчас достаточно одного клика на ссылку, чтобы подвергнуть данные пользователей и организаций риску вторжения. Фишинговые атаки часто маскируются под пользователей сети, тем самым снижая нашу защиту. Ни одна отрасль промышленности не застрахована от угрозы кибератак.

Фишинг – это метод, используемый для компрометации компьютеров и кражи конфиденциальной информации у частных лиц, притворяясь электронной почтой или веб-сайтом доверенной организации. Хакеры ищут пароли, номера кредитных карт, информацию о банковских счетах – или любую информацию, которая может быть использована для доступа к данным.

Большинство успешных фишинговых кампаний заканчиваются тем, что пользователь загружает вредоносное ПО в свою систему.

Эксперты компании Positive Technologies проанализировали кибератаки в первом квартале 2020 года и выяснили, что число инцидентов значительно выросло по сравнению с предыдущим кварталом. По данным исследования, в первом квартале 2020 года было выявлено на 22,5% больше кибератак, чем в четвертом квартале 2019 года. В общей сложности в течение квартала высокую активность проявляли 23 АРТ-группировки, атаки которых были направлены преимущественно на государственные учреждения, промышленные предприятия, финансовую отрасль и медицинские организации. Так, каждая 10 атака шифровальщиков была направлена на промышленность. На рис. 1 представлено процентное соотношение устройств и видов пользователей, подвергшихся атакам

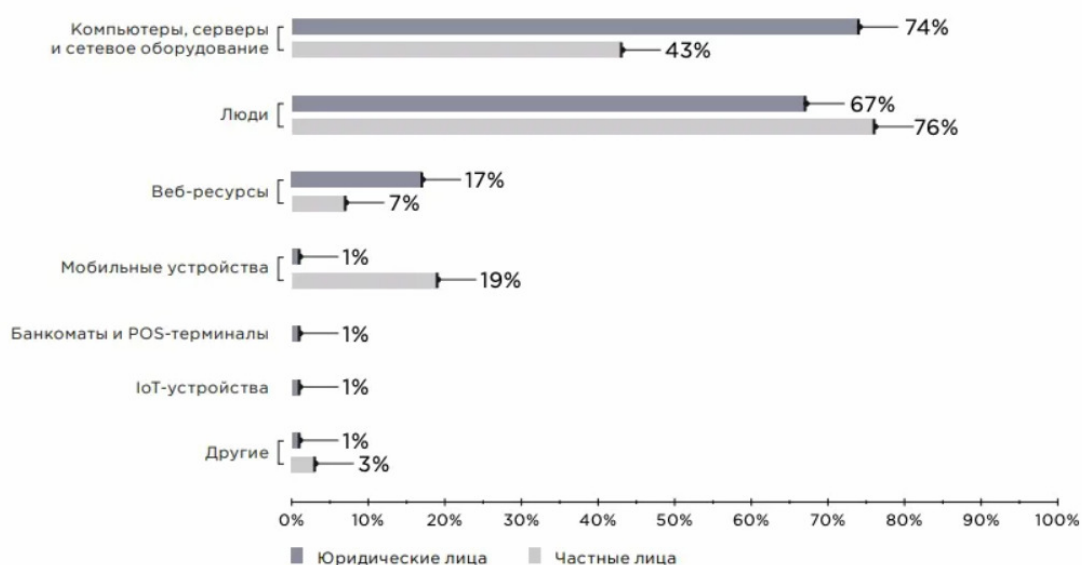


Рис. 1. Распределение фишинговых атак

Распространенные типы фишинговых атак и методы их инициализации. До сих пор фишинг электронной почты остается популярным выбором для большинства злоумышленников. Он заключается в имитации популярного бренда или учреждения, обращающегося к пользователю. Более сложные фишинговые электронные письма делают адрес отправителя совпадающим с адресом людей или компаний, с которыми вы регулярно общаетесь. Они содержат вредоносные вложения или ссылки, предназначенные для доставки вредоносных программ на ваше устройство.

Кибератаки используют *Target*-технику, чтобы нацелиться на конкретные предприятия. Они выходят за рамки рассылки массовых электронных писем или заполнения случайных сайтов рекламой. Подмножеством и высокоэффективной формой фишинговой атаки является фишинговая атака «с копьем», в ходе которой хакер исследует предполагаемую цель и включает в электронное письмо детали, которые делают его более достоверным. Эти сведения могут, например, ссылаться на корпоративное социальное мероприятие предыдущего месяца, опубликованное на общедоступном веб-сайте. Защита от такого рода атак может быть чрезвычайно сложной.

Метод клонирования включает в себя имитацию надежного сайта, который часто посещает пользователь. Люди получают электронные письма, предупреждающие их о проблеме с их учетной записью. Хакеры создают целый вредоносный сайт, который выглядит как тот, на который регулярно заходит пользователь. Злоумышленники надеются обмануть пользователей, предоставив им личные учетные данные.

Фишинговые атаки, как правило, преследуют большой пул целей на таких платформах, как Facebook или других сайтах социальных сетей. Информация, которую люди предоставляют, может показаться пустяком, но этого достаточно, чтобы получить доступ к паролям пользователей и взломать данные учетной записи.

Как предотвратить фишинг

Существует несколько различных технологических подходов к борьбе с фишинговыми атаками. Некоторые продукты отправляют тестовые фишинговые электронные письма корпоративным сотрудникам, которые затем предоставляют руководству по безопасности показатели эффективности своих программ обучения борьбе с фишингом. Качество их, естественно, может варьироваться.

Другой технологический подход заключается в использовании эвристического продукта для определения того, является ли электронное письмо мошенническим. Вероятность успеха этих решений неоднозначна. Они отфильтровывают многие из очевидных мошенничеств, но оставляют нетронутыми более умно оформленные электронные письма. Помимо попыток контролировать эксплойты социальной инженерии, компании также могут управлять рисками, инвестируя в страхование ответственности за кибербезопасность.

Таким образом, можно заключить, что техника фишинга, вероятно, является одной из самых простых и трудных вещей, которые можно остановить,

потому что этот тип атаки основан на отправке кучки случайных писем и тем самым заставляет людей нажимать на ссылку, которая открывает целую франшизу уязвимостей. Также существуют «фишинг-копья», которые представляет собой высоко персонализированные электронные письма, которые переадресовываются человеку, занимающему более высокую должность в организации, который имеет больший доступ, чем типичные цели фишинговой электронной почты.

Советы о том, как избежать фишинга, состоят из нетехнических гарантий, поскольку пользователь должен нажать на ненадежный источник, который входит через внешнюю среду. Лучший, а иногда и единственный способ решить эту проблему – это показать сотрудникам, как читать электронную почту, тем самым уменьшая реакцию коленного рефлекса.

Список литературы

[1]. *Масалков А.М.* Особенности киберпреступлений. Инструменты нападения и защита информации: учебное пособие/ А.М. Масалков.– М:ДМК Пресс, 2018. – 211 с.

[2]. *Таненбаум Э., Уэзеролл Д.* Компьютерные сети. 5-е изд. – СПб.: Питер, 2016. – 960 с

[3]. *Тарасов А.А.* Функциональная устойчивость информационных систем: проблемы и пути их решения // Вопросы защиты информации. – 2012. – № 4. – С. 73-80

Бандурина Екатерина Михайловна – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: bandurinakatya7@yandex.ru

ПРИМЕНЕНИЕ АВТОМАТИЧЕСКОГО СКАНЕРА ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ СЕТИ

Введение. Сохранность конфиденциальных данных – одна из основополагающих задач для обеспечения успешной работы каждого предприятия. Ежегодно всё больше компаний внедряют в использование способ организации работы посредством использования электронного документооборота. Помимо явных преимуществ в виде ускорения и автоматизации большинства процессов, такой подход подразумевает ряд особенностей, связанных с необходимостью защитой от уязвимостей, воспользовавшись которыми мошенники могут получить доступ к конфиденциальной информации. Поэтому становится актуальным вопрос минимизации вероятности разглашения данных посредством мошенничества с использованием уязвимости в программных продуктах.

Обоснование необходимости сканирования уязвимости. Уязвимостью называется параметр, отвечающий за наличие в сети или приложениях несовершенств, воспользовавшись которыми, злоумышленники могут навредить работе приложения или заполучить хранящиеся в нём данные.

Поскольку предприятия работают, используя целый ряд программного обеспечения, то необходимо систематически проверять его на наличие уязвимостей.

Существуют несколько методов определения уязвимости: сканирование и тестирование на проникновение. Первый метод позволяет получить список возможных уязвимостей и производить их дальнейшую обработку. Его преимущество заключается в непрерывном и автоматическом выполнении с меньшими затратами ресурсов. Второй – определяет уязвимости и производит проверку на проникновение посредством моделирования кибер-атаки, выполняется продолжительное время и затрачивает наибольшее по сравнению со сканированием число ресурсов.

Поскольку процесс оценки уязвимости служит хорошим базисом для дальнейшего тестирования на проникновение, то программный продукт, использующийся для сканирования и обработки уязвимостисети, должен обеспечивать наилучший функционал.

Причины появления уязвимостей. Существует множество способов, воспользовавшись которыми мошенники могут взломать сеть, получив, тем самым, доступ к конфиденциальной информации. Однако можно выявить основные причины появления уязвимостей [1]:

1. Отсутствие обновлений ПО: для исправления выявленных ошибок в работе программных продуктов, разработчики выпускают обновления. Соответственно, их несвоевременная установка приводит к тому, что данной уязвимостью могут воспользоваться мошенники.

2. Недостаточная сегментация сети и конфигурация программ: сложность структуры сети может стать причиной наличия недостатков в её архитектуре, а неправильная конфигурация программ – вызывает дополнительные бреши в безопасности.

3. Использование незащищённых соединений: данная уязвимость может появиться из-за просрочки сертификатов SSL / TLS.

4. Наличие неопознанных или неуправляемых объектов в сети: поэтому важно убедиться, что лишь одобренные устройства имеют доступ к портам сети.

5. Наличие сторонних приложений: поскольку стороннее приложение может получить несанкционированный доступ к вашему, создавая, тем самым, дыры в безопасности.

6. Небезопасный код: наибольшую распространённость при утечке данных получили SQL-инъекции, внедряемые в запросы к базе данных.

7. Недостаточное управление привилегиями: для минимизации возможной утечки конфиденциальной информации, привилегии пользователей должны быть строго разграничены.

Сканеры уязвимостей. Поскольку определение уязвимостей является первоочередной задачей в процессе борьбы с ними, то наилучшим вариантом будет использование специализированного программного обеспечения для проверки ресурсов сети, работающих портов и устройств, операционной системы и имеющихся приложений.

Хороший сканер уязвимостей должен позволять не только выявлять проблемы в безопасности, но и оценивать их приоритет. На основе данной оценки администратор выстраивает работу над уязвимостями. В рамках данной статьи рассмотрим наиболее популярное программное обеспечение для сканирования уязвимостей, которые предлагают бесплатную пробную версию.

После устранения уязвимостей важно наличие автоматически составляющегося составления отчёта о состоянии безопасности сети.

Были выбраны 4 наиболее популярных [2] программных продукта, функционал которых полностью удовлетворяет описанным выше требованиям:

1. Nessus. Его особенностью считается то, что программа не делает предположений о конфигурации сервера и производит проверку всех имеющихся портов. Открытый исходный код позволяет системе прозрачно работать, а администратору - изменять исходный код по своему усмотрению. К преимуществам относят ежедневно обновляемый список уязвимостей.

2. IBM Security QRadar. Для непрерывного поиска и обнаружения уязвимостей обеспечивают управление уязвимостями в реальном времени. Пользователь также имеет возможность изменить существующие поисковые фильтры, либо создать новые.

3. BurpSuite. Использует методы определения местоположения для определения провалов, создаваемых современными приложениями, которые могут поглощать запросы. Методология, разработанная с учетом соотношения сиг-

нал/шум, максимизирует охват, сводя к минимуму количество ложных срабатываний, возвращаемых пользователю.

4. Acunetix Vulnerability Scanner. Для повышения эффективности сканирования позволяет использовать несколько локально развернутых модулей. Работа может производиться как с локальной, так и с облачной версией Acunetix.

С помощью G2, сайта с возможностью для сравнения сканеров уязвимостей на основе отзывов пользователей, проведём сравнение выбранных программных продуктов по некоторым наиболее важным характеристикам (см. рис.1).

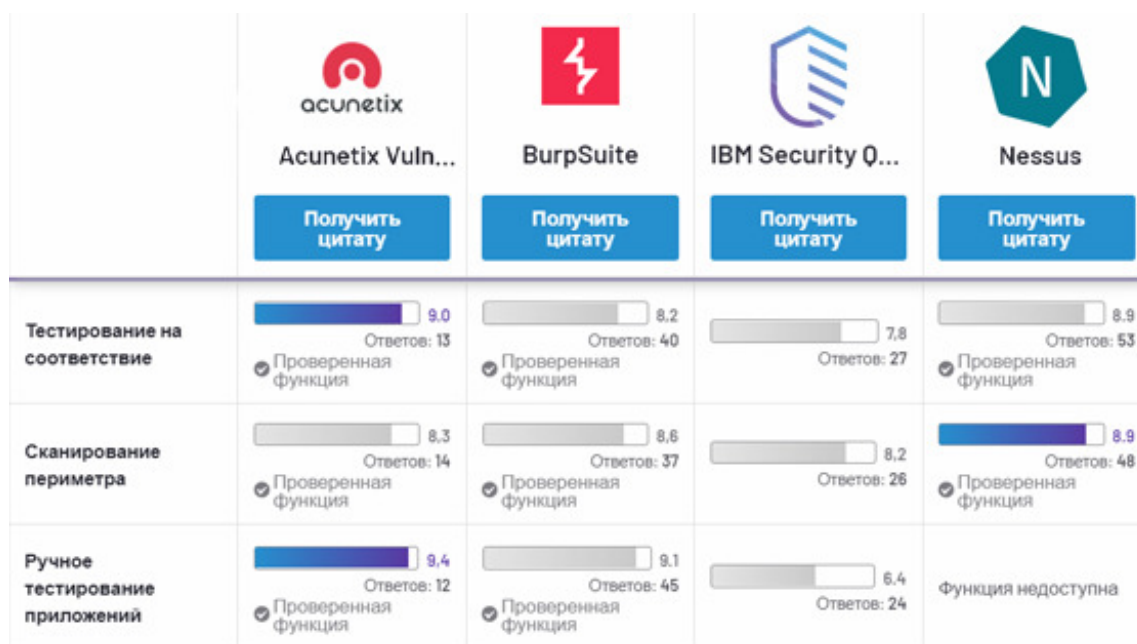


Рис.1. Сравнительный анализ наиболее важных параметров

Исходя из данного сравнения можно сделать вывод, что в каждом сканере уязвимостей есть как сильные, так и слабые стороны. Поэтому в выборе следует основываться на приоритетный функционал и дальнейшие особенности использования.

Заключение. Не смотря на пользу использования сканеров уязвимости [3] для определения возможных пробелов в безопасности, необходимо помнить, что работа сканера сопряжена с вторжением в работающий код целевых устройств. Данное вторжение может привести к ошибкам или перезагрузкам. В некоторых сетях сканеры занимают полосу пропускания и могут вызывать общие проблемы с производительностью. На рынке существует множество типов программных средств безопасности, однако использование программного обеспечения для сканирования уязвимостей является важным первым шагом на пути к защите сети. Выбор конкретного программного обеспечения следует производить исходя из наиболее приоритетных функций, поскольку каждое программное обеспечение имеет как сильные, так и слабые стороны.

Список литературы

[1] *Топ-15* платных и бесплатных инструментов для сканирования уязвимостей в 2020 году [Электронный ресурс]// Компания DNSstuff: сайт – Режим доступа: <https://www.dnsstuff.com/network-vulnerability-scanner> (дата обращения 12.10.2020)

[2] *Лучшее* программное обеспечение для сканирования уязвимостей [Электронный ресурс] // Рынок технологий G2: сайт – Режим доступа: <https://www.g2.com/categories/vulnerability-scanner#:~:text=Vulnerability%20scanners%20are%20tools%20that,scans%20to%20identify%20potential%20exploits> (дата обращения 15.10.2020)

[3] *Сканеры* уязвимостей. Взгляд со стороны вендора и со стороны пользователя [Электронный ресурс] // Журнал по информационной безопасности: сайт – Режим доступа: <http://lib.itsec.ru/articles2/networks/skanery-uyazvimosteyvzglyad-so-storony-vendora-i-so-storony-polzovatelya> (дата обращения 16.10.2020)

Артемова Анна Александровна – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: AnArtAl@mail.ru

Литвиненко Александра Андреевна – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: alexandralitvinenko1998@gmail.com

Ерохин Илья Игоревич – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: drleiter@rambler.ru

СРЕДСТВА И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Введение. Система защиты информации в электронном документообороте – это совокупность направлений, методов, средств и мероприятий, препятствующих несанкционированному доступу к информации, её разглашению или утечке. Основной характеристикой системы является её комплексность, то есть наличие в ней обязательных элементов, охватывающих все направления защиты информации. Исходя из ценности передаваемой информации, определяются средства и методы защиты. Для обеспечения информационной безопасности электронного документооборота используются технические, программные, организационно-правовые и криптографические средства.

Технические (аппаратные) средства. К аппаратным средствам относятся: сетевые фильтры, генераторы шума, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Основными методами реализации аппаратных средств являются следующие:

1. Физическое разграничение сетевого оборудования;
2. Автоматическое создание резервных копий;
3. Использование межсетевых экранов и маршрутизаторов.

К достоинствам технических средств относятся высокая надежность, возможность создания развитых комплексных систем защиты. Недостатки: высокая стоимость, необходимость регулярного проведения регламентных работ и контроля [1].

Программные средства. К программным средствам относятся: программы контроля доступа, шифрования информации, для идентификации пользователей, удаления временных файлов, тестового контроля системы защиты и другие. Наиболее приемлемыми для реализации программных средств являются следующие методы:

1. Логическое разграничение сети;
2. Использование антивирусного ПО;
3. Использование программных средств идентификации и аутентификации пользователей.

Достоинства программных средств – это надежность, гибкость, универсальность, простота установки, способность к модификации. Недостатки: возможность несанкционированного изменения, расходование ресурсов компьютерных систем, ограниченная функциональность сети [2].

Организационно-правовые средства. С помощью организационно-правовых средств защиты регламентируются и реализуются права на информацию, производится контроль за соблюдением прав в процессе деятельности исполнителей на нормативно-правовой основе. При этом используются следующие организационные методы:

1. Предоставление прав доступа в соответствии с должностью;

2. Введение учета ознакомления сотрудников с информацией ограниченного распространения;

3. Организация учета ключей шифрования и подписи, их хранения, эксплуатации и уничтожения.

Преимущества организационно-правовых средств защиты: универсальность, широкий круг решаемых задач, гибкость реагирования на несанкционированные действия, возможность изменения.

Недостатки: зависимость от субъективных факторов, низкая надежность [3].

Криптографические средства. Криптографическими средствами защиты называются специальные средства и методы преобразования информации, в результате которых маскируется её содержание. Наиболее распространенными методами являются алгоритмы открытых ключей для обеспечения подлинности и целостности информации и использование цифровых сертификатов.

Достоинство криптографических средств защиты – это высокая гарантированная стойкость защиты. Недостатки: значительные затраты ресурсов, высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены, трудности совместного использования зашифрованной информации [4].

Выводы. Таким образом, в статье были рассмотрены аппаратные, программные, организационно-правовые и криптографические средства защиты информации, выявлены их основные достоинства и недостатки. Для обеспечения информационной безопасности электронного документооборота необходимо применение описанных средств защиты в совокупности.

Список литературы

[1]. *Защита систем электронного документооборота*/ [Электронный ресурс]. Режим доступа: <https://wiseadvice-it.ru/o-kompanii/blog/articles/zashhita-sistem-edo/> (дата обращения: 03.08.2020).

[2]. *Особенности защиты электронного документооборота*/ [Электронный ресурс]. Режим доступа: <https://novainfo.ru/article/2747> (дата обращения: 10.08.2020).

[3]. *Даниленко А.Ю.* Безопасность систем электронного документооборота. Технология защиты электронных документов. Серия: Основы защиты информации. – 2020.

[4]. *Защита электронного документооборота* / [Электронный ресурс]. Режим доступа: <https://tvoi.biz/dokumenty/elektronnyj-dokumentoorot/zashhita-elektronnogo-dokumentoorot.html> (дата обращения: 15.08.2020).

Сальникова Анна Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: hearofletters@yandex.ru

Твердова С.М. –

ТЕХНОЛОГИЯ DLP

Утечка данных является одной из самых опасных угроз в киберпространстве. Она являет собой действия отдельных лиц, которым удалось заполучить легитимные права доступа у информации, что привело к нарушению её конфиденциальности. Такие действия можно разделить на две группы: преднамеренные, которые включают в себя саботаж и промышленный шпионаж, а также случайные - такие, как халатность и незнание [1].

Что делать, если произошла утечка данных. Все зависит от масштабов проблемы. Если в сети оказались имена или адреса, то с этим уже ничего не поделаешь. Но когда речь идет о доступе к каким-то приложениям (например, утекли адреса и пароли почтового сервиса), в этом случае нужно срочно принимать меры.

В первую очередь необходимо зайти в свой аккаунт и сразу же сменить пароль. Если такая же комбинация стоит в других сервисах – заменить её и там. По возможности лучше включить двухфакторную аутентификацию.

В случае с банковскими утечками остается лишь быть начеку: к вам в любой момент могут позвонить мошенники и представиться банковским сотрудником. В подтверждение своих слов они нередко озвучивают всю информацию о клиенте, включая остаток средств на счете – данные такого типа у злоумышленников тоже могут быть. В таком случае лучше повесить трубку и перезвонить в банк самостоятельно.

Как предотвратить утечки данных. Существует несколько методов и процедур безопасности, которые необходимо применить, чтобы свести к минимуму риск утечки данных. Конечно, невозможно проконтролировать все – мишенью киберпреступника можно стать в любой момент. Тем не менее, принятие нескольких превентивных мер придаст немного спокойствия.

Необходимо иметь резервные копии важных данных или информации на непредвиденный случай. К личным устройствам и данным должны иметь доступ только те люди, которым можно доверять. Таким образом можно избежать умышленных утечек. Рекомендуется использовать фильтры спама и фишинга, чтобы снизить риск успешных атак социальной инженерии. Также важно использовать брандмауэры для защиты сети от вредоносных программ, таких как вымогатели, шпионские программы или кейлоггеры. VPN с надежным шифрованием обеспечит безопасность подключений, а надежные пароли и двухфакторная аутентификация пригодятся для наиболее конфиденциальных учетных записей. Также использование генератора сложных паролей гарантирует безопасность хранения личных данных.

Для предотвращения утечек информации, многие компании используют технологию DLP, позволяющую в автоматическом режиме организовывать

проверку информационных потоков, обнаруживать в них конфиденциальные данные, и в итоге применять к ним определенные действия (в большинстве случаев осуществлять блокировку передачи данных).

Общая характеристика DLP. DLP-система (от английского Data Leak Prevention) это специализированное ПО, которое защищает организацию от утечек данных. Данная технология – не только возможность заблокировать передачу конфиденциальной информации по различным каналам, но и инструмент для наблюдения за ежедневной работой сотрудников, который позволяет найти слабые места в безопасности до наступления инцидента.

Лингвистический анализ. Толчок в разработке лингвистических технологий был сделан в начале этого века создателями email-фильтров. Прежде всего, для защиты электронной почты от спама. Это сейчас в антиспамовских технологиях преобладают репутационные методы, а в начале века шла настоящая лингвистическая война между снарядом и броней - спамерами и антиспамерами. Например, простейшие методы для обмана фильтров, базирующихся на стоп-словах с заменой букв или добавления дополнительных символов (секретно, написанное на транслите, например) [2]. Антиспамеры довольно быстро научились бороться с такими хитростями, но тогда появился графический спам и прочие хитрые разновидности нежелательной корреспонденции.

Однако использовать антиспамерские технологии в DLP-продуктах без серьезной доработки невозможно. Ведь для борьбы со спамом достаточно делить информационный поток на две категории: спам и не спам. Метод Байеса, который используется при детектировании спама, дает только бинарный результат: «да» или «нет». Для защиты корпоративных данных от утечек этого недостаточно – нельзя просто делить информацию на конфиденциальную и неконфиденциальную. Нужно уметь классифицировать информацию по функциональной принадлежности (финансовая, производственная, технологическая, коммерческая, маркетинговая), а внутри классов – категоризировать её по уровню доступа (для свободного распространения, для ограниченного доступа, для служебного использования, секретная, совершенно секретная и так далее) [3].

Большинство современных систем лингвистического анализа используют не только контекстный анализ (здесь имеется в виду, в каком контексте, в сочетании с какими другими словами используется конкретный термин), но и семантический анализ текста. Эти технологии работают тем эффективнее, чем больше анализируемый фрагмент. На большом фрагменте текста точнее проводится анализ, с большей вероятностью определяется категория и класс документа. При анализе же коротких сообщений (SMS, интернет-пейджеры) ничего лучшего, чем стоп-слова, до сих пор не придумано.

Принцип работы DLP. Часто в компаниях больше внимание уделяют внешним угрозам: спаму и фишинг-атакам типа «отказ в обслуживании», ви-

русам (троянскому ПО, червям), подмене главных страниц интернет-ресурсов, шпионскому и рекламному программному обеспечению, социальному инжинирингу. Но на самом деле внутренние угрозы способны причинить компании куда более серьезный ущерб, чем злоумышленники за её пределами.

В принципе любой работник компании может являться потенциальным инсайдером и поставить информационную безопасность под угрозу. От злого умысла или банальной оплошности не застрахован никто: от низшего звена и до топ-менеджмента.

Принцип работы DLP-системы прост и заключается в анализе всей информации: исходящей, входящей и циркулирующей внутри компании. Система при помощи алгоритмов анализирует, что это за информация и в случае, если она критичная и отправляется туда куда ей не положено - блокирует передачу и/или уведомляет об этом ответственного сотрудника.

Основу DLP составляет набор правил. Правила могут быть любой сложности и касаться разных аспектов работы. Если кто-то их нарушает, то ответственные лица получают уведомление.

Система отслеживает не только время работы и активные программы на компьютере, но и любую другую работу с информацией, в частности, ввод данных с клавиатуры, переписку и передачу файлов по почте, в соцсетях и мессенджерах, отправляемые на печать документы, время простоя, SIP-телефонию, активность на сайтах и многое другое.

Способы перехвата данных DLP. Для анализа данных необходимо, чтобы DLP-система их получила [4].

Есть два основных способа перехвата - серверный и агентский. В первом случае система контролирует сетевой трафик на сервере, через который компьютеры «общаются» с внешним миром. Во втором случае специальные небольшие программы (агенты) устанавливаются на все компьютеры организации и передают с каждой машины данные для анализа.

Агентский перехват является более распространённым, ведь с его помощью можно получить гораздо больше данных из различных каналов коммуникации, а значит и надежнее предотвратить возможные утечки.

Неочевидное использование DLP. Казалось бы, система, созданная для контроля утечки данных, больше ничем не может быть полезна. Однако современные DLP имеют и другие возможности, неочевидные на первый взгляд:

– анализ загруженности персонала. Многие DLP-системы способны вести учет рабочего времени сотрудников. Рабочий процесс каждого пользователя можно представить в виде статистики, которая позволяет проанализировать, насколько сотрудник вовлечен в трудовой процесс;

– обеспечение юридической поддержки. Задача DLP состоит не только в том, чтобы предотвратить утечки, но еще и при наличии судебного разбирательства, предоставить доказательства злоумышленной деятельности;

– использование DLP как инструмента мотивации. Когда сотрудники осознают, что их трудовая деятельность находится под мониторингом, появляется большая ответственность за рабочий процесс. И это в свою очередь приводит к улучшению климата в коллективе;

– использование DLP в качестве хранилища. DLP-технология гарантирует сохранность всей информации, поскольку содержит в своём архиве все коммуникации сотрудников, к которым в случае необходимости можно будет обратиться.

Достоинства DLP. Например, для детектирования цитаты нужен объект-образец. И статистические методы могут с хорошей точностью (до 100%) сказать, есть в проверяемом файле значимая цитата из образца или нет. То есть система не берет на себя ответственность за категоризацию документов - такая работа полностью лежит на совести того, кто категоризировал файлы перед снятием отпечатков. Это сильно облегчает защиту информации в случае, если на предприятии в некотором месте (местах) хранятся нечасто изменяющиеся и уже категоризированные файлы. Тогда достаточно с каждого из этих файлов снять отпечаток, и система будет, в соответствии с настройками, блокировать пересылку или копирование файлов, содержащих значимые цитаты из образцов.

Независимость статистических методов от языка текста и нетекстовой информации - тоже неоспоримое преимущество. Они хороши при защите статистических цифровых объектов любого типа, например, картинок, аудио/видео, баз данных[5].

Недостатки DLP. Простота обучения системы (указал системе файл, и он уже защищен) перекладывает на пользователя ответственность за обучение системы. Если вдруг конфиденциальный файл оказался не в том месте либо не был проиндексирован по халатности или злему умыслу, то система его защищать не будет. Соответственно, компании, заботящиеся о защите конфиденциальной информации от утечки, должны предусмотреть процедуру контроля того, как индексируются DLP-системой конфиденциальные файлы.

Еще один недостаток – физический размер отпечатка. Автор неоднократно видел впечатляющие пилотные проекты на отпечатках, когда DLP-система со 100% вероятностью блокирует пересылку документов, содержащих значимые цитаты из трехсот документов-образцов. Однако через год эксплуатации системы в боевом режиме отпечаток каждого исходящего письма сравнивается уже не с тремя сотнями, а с миллионами отпечатков-образцов, что существенно замедляет работу почтовой системы, вызывая задержки в десятки минут.

Заключение. На вопрос «Нужна ли DLP организации?» можно ответить кратко - да. У каждой компании есть информация, которая имеет ценность, а значит притягивает злоумышленников, не только снаружи, но и изнутри. Это может быть клиентская база, особенности технологических процессов, черте-

жи, даже банальный список адресов для пресс-релиза несет ценность, которую не хочется просто так дарить конкурентам.

Список литературы

[1]. *Афанасьев А.А., Веденьев А.Т., Воронцов А.А., Газизова Э.Р.* Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. – М.: Горячая линия-Телеком, 2012. – 550 с.

[2]. *Белов Е.В., Лось В.П., Мещеряков Р.В., Шелупанов А.А.* Основы информационной безопасности. – М.: Горячая линия-Телеком, 2011. – 558 с.

[3]. *Бражкина Е.Е.* Информационно-психологическая безопасность и манипулирование информацией СМИ // Успехи в химии и химической технологии. – 2012. – № 9(138) том 26. – С. 17–21.

[4]. *Муценек В.Е.* Дезинформация как инцидент информационной безопасности // Известия Иркутского государственного университета. – 2018. – № 24. – С. 24-32.

[5]. *Хроколов В.А.* Безопасность личности, общества и государства: информационно-психологический аспект. // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. – 2018. – № 1. – С. 27–35.

Ерохин Илья Игоревич – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: drleiter@rambler.ru

Климушина Дарья Викторовна – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: lovely_jelly@mail.ru

ТРЕХФАКТОРНАЯ АНОНИМНАЯ СХЕМА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ СРЕД ИНТЕРНЕТА ВЕЩЕЙ

Введение. Интернет вещей (IoT) состоит из узлов с ограниченными ресурсами, что представляется из себя плотно разбросанные узлы в средах Интернета вещей с обеспечением непрерывное обслуживание, независимо от времени и местоположения. В настоящее время IoT был принят для многих приложений, включая здравоохранение, умный дом, умную фабрику и умный город. Кроме того, появление сотовой сети пятого поколения (5G) и её коммерциализация породили ожидание гиперссылочной сети для соединения и обмена информацией не только между отдельными портативными терминалами, но и между большинством (если не всеми) объектами, которые мы используем в повседневной жизни. Согласно исследованию [1] к 2020 году около 50 миллиардов сенсорных устройств по всему миру будут подключены к сетям Интернета вещей, и ожидается, что число этих устройств будет экспоненциально расти с коммерциализацией сетей 5G. Согласно требованиям 5G-vision сектора стандартов радиосвязи Международного союза электросвязи, массивная сеть Интернета вещей вмещает около 1 миллиона объектов на км².

Развитие Интернета вещей и массового Интернета вещей имеет огромный потенциал, но эти среды подвергают устройства широкому спектру уязвимостей из-за увеличения поверхности атаки. Поэтому для защиты конфиденциальности пользователей в средах Интернета вещей необходимо обеспечить такие свойства безопасности, как

- безопасность данных;
- безопасность виртуальной сети;
- доступность услуг;
- целостность данных.

В сетевой архитектуре механизмы безопасной аутентификации пользователей и распределения ключей с использованием криптографии должны поддерживать эти требования безопасности Интернета вещей [4]. В Сети интернета вещей пользовательские узлы и сенсорные узлы, взаимодействующие друг с другом, подвергаются различным угрозам.

Когда секретные ключи открыты, весь трафик в сети может быть расшифрован. Даже когда ключ, хранящийся в физической памяти, подвергается атаке через боковой канал, схема аутентификации пользователя должна реализовывать контрмеры, которые предотвращают вторжение злоумышленника в сеть Интернета вещей и получение контроля над ней. Механизм отзыва – это простая и эффективная контрмера. При внедрении механизма отзыва, когда личный ключ пользователя теряется или крадется, администратор выдает новый ключ пользователю.

Сетевая модель и процесс аутентификации. В настоящее время для обеспечения безопасности, масштабируемости и эффективной вычислитель-

ной стоимости используются различные модели архитектуры Интернета вещей [2]. Процесс аутентификации пользователя выглядит следующим образом:

1) MN_i отправляет запрос на вход и аутентификацию в N_j для доступа к сети Интернета вещей.

2) После получения сообщения запроса N_j отправляет полученный запрос в GW для аутентификации MN_i .

3) GW проверяет сообщение, полученное от N_j , аутентифицирует MN_i и отвечает на N_j .

4) N_j посылает ответ MN_i , а затем MN_i и N_j взаимно устанавливают ключ сеанса с помощью аутентификации.

Био-хэш-функция. Биометрия предоставляет уникальный метод идентификации для устранения уязвимостей безопасности в определенных учетных данных пользователей, которые могут быть забыты или украдены, таких как пинкоды, пароли и токены. Биометрические характеристики отпечатка незначительно изменяются при каждом вводе по различным причинам, таким как сухая или потрескавшаяся кожа, или наличие пыли на датчиках отпечатка [3]. Чтобы решить проблему высоких показателей ложного отторжения, в 2004 году был предложен метод двухфакторной аутентификации на основе внутренних продуктов между токенизированными псевдослучайными числами и специфичными для пользователя отпечатками пальцев. Био-хэш-код случайным образом сопоставляет биометрический признак с двоичной строкой, используя специфичный для пользователя маркер псевдослучайных чисел. Био-хэш был применен к целому ряду недавно предложенных схем. Технология био-хэша эффективна для схем многофакторной аутентификации на основе биометрии, поскольку она подходит для устройств малой емкости.

Схема Диллона и Калры. Далее рассмотрим схему аутентификации пользователей Диллона и Калры, которая состоит из трех этапов: регистрации, входа и аутентификации, и фазы смены пароля, а также проведем криптоанализ схемы Диллона и Калры.

В схеме MN_i может одновременно получать идентификатор и пароль, от украденного или потерянного пользователями мобильного устройства. можно выполнять автономные атаки угадывания с помощью следующих процессов:

– извлечение секретных параметров из мобильного устройства пользователя;

– подбор личности кандидата и сравнение извлеченного значения с вычисленным значением другого пользователя;

– выбор пароля кандидата вычисляется и сравниваются два параметра: извлеченное значение с вычисленным значением.

Если измерения показывают, что они совпадают, алгоритм успешно нашел правильную личность и пароль. Иначе, алгоритм запускается снова и повторяет шаги процессов до тех пор, пока не будет найден правильный идентификатор и пароль.

После успешного угадывания MN_iID_i и PW_i через описанный выше процесс, можно не только выполнить атаку, но и также воспользоваться угадан-

ным идентификатором и паролем для доступа к другой системе аутентификации для взлома других конфиденциальных данных пользователя.

Список литературы

[1]. *Внуков А.А.* Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. – 2-е изд., испр. и доп. – М.: Издательство Юрайт, 2018. – 246 с.

[2]. *Казарин О.В.* Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О.В. Казарин, И.Б. Шубинский. – М.: Издательство Юрайт, 2020. – 342 с.

[3]. *Катмаков П.С.* Биометрия : учебное пособие для вузов / П.С. Катмаков, В.П. Гавриленко, А.В. Бушов ; под общей редакцией П.С. Катмакова. – 2-е изд., перераб. и доп. – М.: Издательство Юрайт, 2020. – 177 с.

[4]. *Чернова Е.В.* Информационная безопасность человека : учебное пособие для вузов / Е.В. Чернова. – 2-е изд., испр. и доп. – М.: Издательство Юрайт, 2020. – 243 с.

Бандурина Екатерина Михайловна – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: bandurinakatya7@yandex.ru

СЕКЦИЯ 9.

**ДИНАМИКА, ПРОЧНОСТЬ И НАДЕЖНОСТЬ
ПОДЪЕМНО-ТРАНСПОРТНЫХ,
СТРОИТЕЛЬНЫХ, ДОРОЖНЫХ МАШИН
И ОБОРУДОВАНИЯ**

И.И. Сорокина

К ВОПРОСУ ПРОЕКТИРОВАНИЯ ОРТОГОНАЛЬНОЙ ЧЕРВЯЧНОЙ ПЕРЕДАЧИ С КОСОЗУБЫМ ЦИЛИНДРИЧЕСКИМ КОЛЕСОМ

От качества передач во многом зависят важнейшие показатели механизмов – работоспособность, надёжность, металлоёмкость, себестоимость. Пространственные передачи зацеплением, в том числе червячные широко используются в большинстве современных машин и механизмов и при всём многообразии их конструктивного исполнения содержат сложные рабочие поверхности зацепления, геометрическая оптимизация которых до сих пор ведется.

При проектировании червячного мотор-редуктора в условиях не достаточного технического оснащения производства и ввиду сложности изготовления червячного колеса было предложено организовать передачу с конвалютоночервяка на косозубое цилиндрическое колесо. При этом реализация подобного зацепления привела к поломке 80% зубьев колеса, износ носил прочностной характер.

Задачей исследования был поиск возможных причин такого разрушения и выдача рекомендаций по расчету и проектированию подобного соединения.

Проведя обзор доступной литературы, стоит отметить, что передачи такого типа не являются нововведением. Однако, их расчет и изготовление сопряжены с определенными трудностями. В ряде справочников, например, [1] подобные передачи предлагалось проектировать как скорректированные винтовые передачи с малым числом зубьев шестерни. В этом случае активные поверхности витков червяка и зубьев колеса получаются эвольвентными винтовыми с равным нормальным модулем. Второй вариант проектирования подобной передачи, рассмотренный, например в [2], состоит в том, что червяк проектируется, как эвольвентный, со стандартным осевым модулем, которому должен быть равен торцовый модуль колеса. В обоих расчетных случаях модуль принимает не стандартные значения и такая передача трудно реализуема с технологической точки зрения, что совершенно не отвечает задачам проводимого исследования.

Учитывая, что для сопряженности червячной передачи необходимо и достаточно, чтобы у червяка и червячной фрезы, нарезающей зубья колеса, были равны между собой основные шаги, авторами [3] предлагается достаточно простой алгоритм расчета подобной передачи с учетом сопряженности активных поверхностей звеньев рассматриваемой передачи. Основное преимущество этого расчета его простота и доступность, он может быть реализован в среде КОМПАС-3D в библиотеке «Валы и механические передачи». Конструктор задается параметрами фрезы для нарезания колеса, осевой модуль червяка выбирается исходя из параметров станка, а соблюдение заданного межосевого расстояния достигается высотной коррекцией зубьев колеса. Таким об-

разом, провести расчет подобной передачи в условиях производства довольно просто.

Анализируя доступные источники, следует отметить, что во всех рассматриваемых работах авторы сходятся во мнении, что профиль червяка должен быть эвольвентным. У конволютного червяка (ZN) теоретический торцовый профиль витков очерчен по удлиненной (реже укороченной) эвольвенте. В осевом сечении червяк имеет криволинейный профиль витков, а в нормальном сечении – прямолинейный. У эвольвентного червяка (ZI) теоретический торцовый профиль витков очерчен по эвольвенте круга. В осевом и нормальном сечениях червяк имеет криволинейный профиль витков. Таким образом, эвольвентный червяк представляет собой косозубое цилиндрическое зубчатое колесо с очень большим углом наклона зубьев (угол подъема витков), и малым числом зубьев (число заходов). Вероятно, при использовании конволютного профиля в передаче червяк-косозубое колесо нарушается сопряжённость профилей, что и могло привести к такой значительно поломке.

Кроме того, поверхность червячного колеса выполняют вогнутой с целью повышения нагрузочной способности зацепления, что в свою очередь увеличивает угол охвата червяка и обеспечивает линейный контакт зубьев колеса и витков червяка. Поэтому прочность косозубого колеса в указанных условиях примерно на 40 % ниже, чем у традиционного червячного колеса. Нагрузочная способность червяков всех типов является приблизительно одинаковой.

Таким образом, опираясь на проведенный обзор литературы, можно рекомендовать пересчет параметров передачи мотор-редуктора в среде КОМПАС-3D, библиотека «Валы и механические передачи». Профиль червяка выполнить эвольвентным, прочность колеса повысить за счет грамотного выбора применяемого материала.

Список литературы

[1]. *F.L. Litvin, A. Fuentes. Gear Geometry and Applied Theory of Gearing* (2nd edition). Cambridge University Press, 2004, 800 pp.

[2]. *Курлов Б.А.* Винтовые эвольвентные передачи: Справочник. – М: Машиностроение, 1981.-176с.

[3]. *Лагутин С.А., Гудов Е.А.* Червячные механизмы с винтовым движением звеньев // Теория Механизмов и Машин. – 2008. – №1. – Том 6. – С.89-98.

Сорокина Ирина Игоревна – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: sorokina-i@yandex.ru

МЕТОД РАСШИФРОВКИ КАНАТА И ОЦЕНКИ ЕГО ПРОЧНОСТИ

При эксплуатации канатов бывают случаи, когда в наличии есть канат, марка и прочность которого неизвестны.

Цель работы: создать методику расшифровки типа каната и определения прочности каната.

Исследование разрывной прочности каната осуществляют с помощью настольного экспериментального устройства (рис. 1), которое состоит из основания 1 и ворот 2 для закрепления концов исследуемой проволоки 3. При растяжении проволоки возникает деформация тензометрической пластины 4. Деформацию измеряют индикатором 5, после чего определяют разрывное усилие с помощью тарировочного графика. Тарировку пластины осуществляют путем последовательного навешивания гирь 8, с помощью блока 6, и гибкого подвеса 7 (условно повернут в плоскость чертежа).

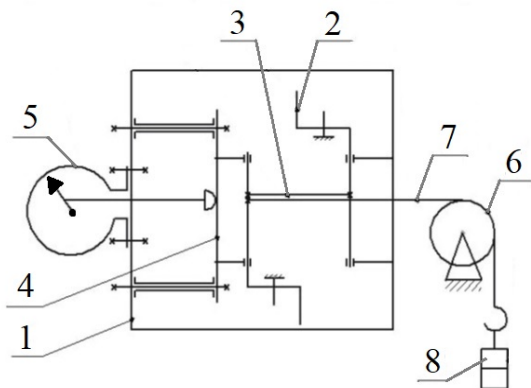


Рис. 1. Устройство для исследования разрывной прочности проволок каната

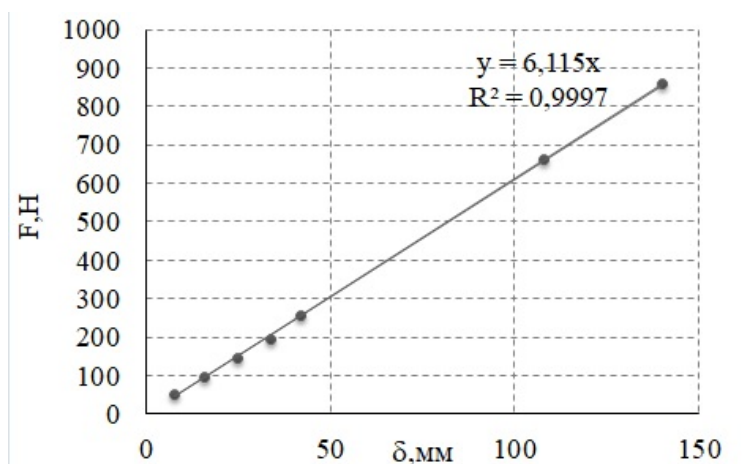


Рис. 2. Тарировочный график

Основными механическими свойствами стальных канатов являются: прочность, модуль упругости, поперечная жесткость, изгибная жесткость, долговечность при огибании блоков и усталостная прочность.

В существующей литературе выделяют три характеристики прочности стальных проволочных канатов: суммарное разрывное усилие проволок P_c , агрегатная прочность P_a (разрывное усилие каната в целом) и конструкционная прочность P_k (агрегатная прочность каната при его эксплуатации в составе конкретного узла).

Суммарное разрывное усилие проволок для каната двойной свивки:

$$P_c = z_n \left(\bar{F}0 + z_1 \bar{F}1 + z_2 \bar{F}2 \right), \quad (1.1)$$

где $\bar{F}0$ – среднее разрывное усилие центральных проволок пряди; $\bar{F}1$ – среднее разрывное усилие толстых проволок; $\bar{F}2$ – среднее разрывное усилие тонких проволок; z_n – число прядей в канате; z_1 – число толстых проволок в пряди; z_2 – число тонких проволок в пряди.

Среднее разрывное усилие проволок:

$$\bar{F} = \sum_{i=1}^n F_i / n = \sum_{i=1}^n \delta_i / n, \quad (1.2)$$

где F_i – разрывное усилие i -й проволоки; n – число исследуемых проволок; k – тарировочный коэффициент тензометрической пластины лабораторного устройства; δ_i – показания индикатора при разрыве i -й проволоки.

Предел прочности проволок каната:

$$\sigma = \frac{\bar{F}}{A}, \quad (1.3)$$

где \bar{A} – средняя площадь поперечного сечения проволок.

$$\bar{A} = \frac{\pi \bar{d}^2}{4}, \quad (1.4)$$

где \bar{d} – средний диаметр проволок.

$$\bar{d} = \sum_{i=1}^n d_i / n. \quad (1.5)$$

Нами взят отрезок каната неизвестной марки длиной 300 мм. Канат расплели, измерили диаметры проволок и разрывные усилия.

Площадь проволоки

$$A_{ц} = \frac{\pi d_{ц}^2}{4} = \frac{3,14 \cdot 0,80^2}{4} = 0,5 \text{ мм}^2;$$

$$A_{ц} = \frac{\pi d_{н}^2}{4} = \frac{3,14 \cdot 0,71^2}{4} = 0,4 \text{ мм}^2;$$

$$A_{ц} = \frac{\pi d_{вн}^2}{4} = \frac{3,14 \cdot 0,39^2}{4} = 0,12 \text{ мм}^2.$$

Предел прочности проволоки:

$$\sigma_{ц} = \frac{F_{ц}}{A_{ц}} = \frac{87,5}{0,5} = 1716,2 \text{ МПа};$$

$$\sigma_{\text{ц}} = \frac{F_{\text{н}}}{A_{\text{н}}} = \frac{67,5}{0,4} = 1657,3 \text{ МПа};$$

$$\sigma_{\text{вн}} = \frac{F_{\text{вн}}}{A_{\text{вн}}} = \frac{26,25}{0,12} = 2157,5 \text{ МПа}.$$

Полученные результаты сведены в табл. 1.

Таблица 1.

Тип проволоки	центральная	наружная	внутренняя
Количество, n шт.	1	9	9
Показания индикатора, мм	0,140	0,108	0,042
Диаметр проволок d , мм	0,80	0,71	0,39
Площадь проволок A , мм ²	0,5	0,4	0,12
Предел прочности, МПа	1716,2	1657,3	2157,5
Разрывное усилие F , кгс	257,5	662,2	858,4

Усреднённый предел прочности проволок каната

$$\sigma = \frac{\sigma_{\text{ц}} + \sigma_{\text{н}} + \sigma_{\text{вн}}}{n} = \frac{1716,2 + 9 \cdot 1657,3 + 9 \cdot 2157,5}{19} = 1897,34 \text{ МПа}.$$

По каталогу [1] найден канат ГОСТ 3077, совпадающий по конструкции со взятым отрезком каната. По таблицам ГОСТ 3077 находим маркировочную группу 190 кгс/мм². Он имеет диаметры: центральной проволоки $d_{\text{ц}} = 0,8$ мм; наружных проволок $d_{\text{н}} = 0,7$ мм; внутренних проволок $d_{\text{вн}} = 0,38$ мм. Это соответствует измеренным значениям (табл. 1).

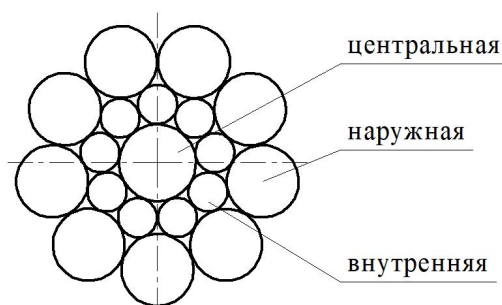


Рис. 3. Схема пряди каната ГОСТ 3077 канат двойной свивки типа ЛК-О конструкции 6х19 (1+9+9)+1 о.с.

Канат грузоподъемный лифтовый ГОСТ 3077, круглопрядный предназначен для подъема людей и грузов. Устойчиво работает в условиях абразивного изнашивания благодаря наличию в наружном слое проволок увеличенного диаметра. Для нормальной эксплуатации требуется несколько повышенный диаметр блоков и барабанов. Применяется для гидравлических лифтов, на лесосплавах, в лесной и деревообрабатывающей промышленности, для лебедок в землеройных и дорожных машинах, в шахтах, в подъемно-транспортных установках [2]. Он используется в качестве подъемных канатов башенных, судовых и автомобильных кранов, для тельферов, в качестве скреперных канатов, тяговых и несущих канатов канатных дорог, барабанных лебедок [3].

Суммарная площадь проволок каната

$$A = \frac{\pi}{4}(d_{\text{ц}} + 9d_{\text{н}} + 9d_{\text{вн}}) = \frac{3,14}{4}(0,8 + 9 \cdot 0,7 + 9 \cdot 0,38) = 8,26 \text{ мм}^2$$

Экспериментально полученное суммарное разрывное усилие

$$F = F_{\text{ц}} + 9F_{\text{н}} + 9F_{\text{вн}} = 858,4 + 9 \cdot 662,2 + 9 \cdot 257,5 = 9135,7 \text{ Н}$$

Отклонение экспериментально полученного разрывного усилия F от суммарного разрывного усилия F_p , заданного в ГОСТ 3077 составляет:

$$\frac{F_p - F}{F_p} \cdot 100\% = \frac{9284 - 9135,7}{9284} \cdot 100\% = 1,6\%,$$

где $F_p = 9284 \text{ Н}$, согласно ГОСТ 3077.

Это отклонение считаем допустимым для экспериментально полученного разрывного усилия каната в условиях учебной лаборатории.

Разрывное усилие каната в целом обычно составляет: $[F] = 0,8F$.

Это значение отличается от указанного в ГОСТ 3077 разрывного усилия каната в целом:

$$\frac{[F] - 0,8F}{[F]} \cdot 100\% = \frac{7592 - 7308,6}{7592} \cdot 100\% = 3,7\%,$$

где $[F] = 7592 \text{ Н}$ – разрывное усилие каната в целом согласно ГОСТ 3077.

Это отклонение приемлемо (не превышает 4%). Считаем канат расшифрованным полностью. Таким образом, с помощью простейшего устройства и несложной методики, может быть расшифрован любой тип каната.

Список литературы

[1]. ГОСТ 3077-80 Канат двойной свивки типа ЛК-О конструкции 6х19 (1+9+9)+1 о.с. Сортамент (с Изменениями № 1, 2). Режим доступа: <http://docs.cntd.ru/document/1200007629> (дата обращения 21.02.2018).

[2]. Ермоленко В.А., Витчук П.В. Особенности расчёта показателей надёжности грузоподъемных машин. – М.: Надежность, 2016. – №2. – 84 с.

[3]. Ермоленко В.А., Степанцов М.А. Конструирование механизма подъема стрелы и груза. // Научно-технические технологии в приборостроении и машиностроении и развитие инновационной деятельности в ВУЗе: Материалы Всероссийской научно-технической конференции – Калуга: Изд-во МГТУ им. Н.Э. Баумана, 2015. – Т.4 – 324 с.

Моргунов Вениамин Валерьевич – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: rise1613@gmail.com

Витчук П.В. –

УНИВЕРСАЛЬНАЯ МАШИНА ДЛЯ ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ АВАРИЙ

В современном мире повсеместно происходят различные природные и техногенные катаклизмы, которые несут за собой ряд разрушений. В большинстве случаев для ликвидации последствий простого человеческого труда недостаточно и необходимо использовать специальную технику, чтобы облегчить человеческий труд и сократить время на ликвидацию последствий. Зачастую происходит так, что специальную технику доставить до места аварии бывает трудно, а иногда и вовсе невозможно ей воспользоваться. Для таких случаев необходимо инновационное решение, а именно универсальная машина для ликвидации последствий.

В качестве базы рассмотрим существующий аналог для ремонтных работ от фирмы Kaiser модель «S12 Allroad» (рис.1) [1]. Машина представляет собой мобильный шагающий экскаватор с полным приводом.

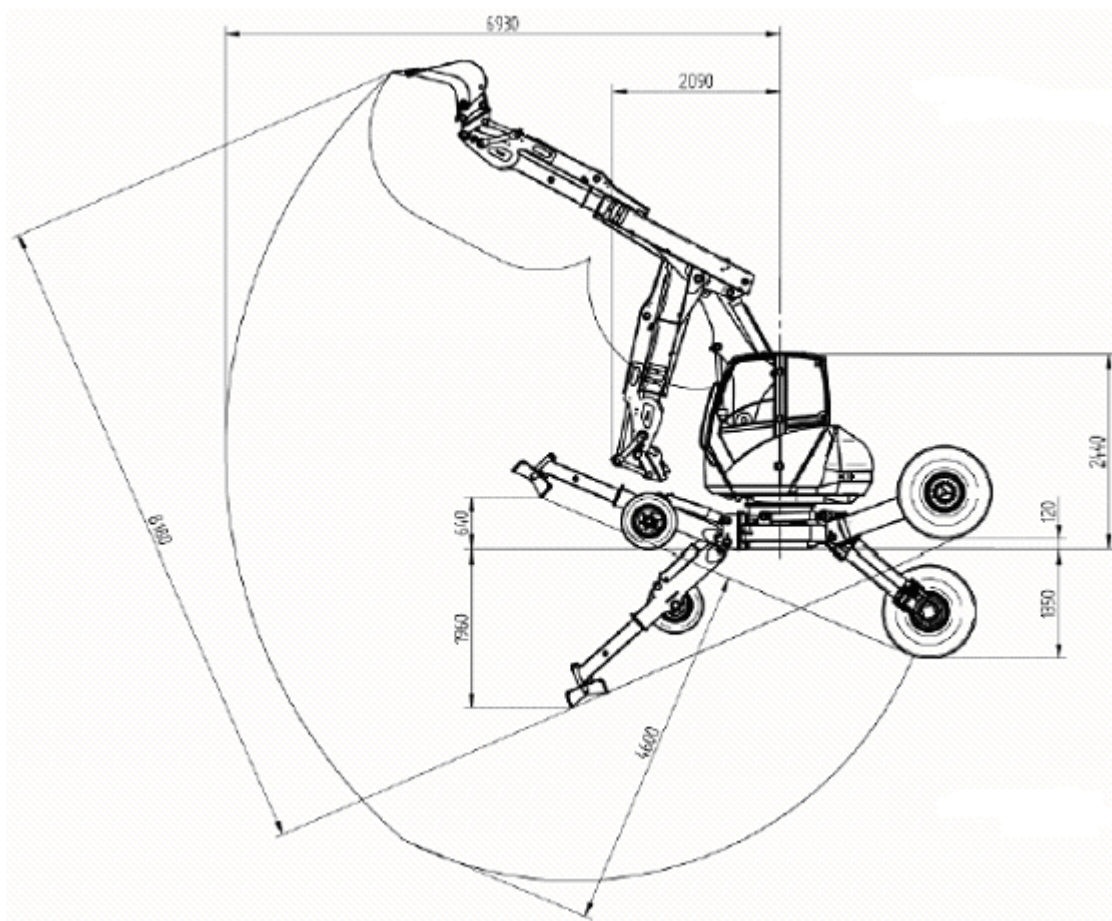


Рис.1.Схема шагающего экскаватора Kaiser

Ходовая часть, специально разработанная для полного привода и управления всеми колесами, а также бесступенчатый гидростатический полный привод обеспечивают оператору исключительную мобильность. Экскаватор имеет возможность перемещения своим ходом, а также возможность передви-

жения по рельсовому пути. Гидравлически регулируемые подушки повышенной проходимости обеспечивают оптимальную устойчивость. В основе S12 Allroad лежит дизельный двигатель Perkins с высокой мощностью и высоким крутящим моментом, а также возможность выбора версии 110 кВт или 129 кВт. Его мощный крутящий момент до 750 Нм уже при 1400 об / мин обеспечивает выдающуюся эффективную работу гидравлической системы [1]. Для увеличения спектра работ на данной модели предусмотрены различные сменные устройства. Например, вместо стандартного ковша на конец стрелы могут устанавливаться: грейфер, рыхлитель, гидромолот и мульчер. Несмотря на внушительную проходимость экскаватор имеет ряд ограничений, связанных с использованием гидравлической системы. Машина не может совершать работы на высоте выше 3500 метров над уровнем моря, а также имеет ряд ограничений по работе в зонах с пониженной температурой.

Изучив технические характеристики данного экскаватора, я пришёл к выводу, что есть возможность устранить данные недостатки и создать новую машину с лучшими техническими характеристиками.

Для передвижения машины можно использовать не только колесный привод, но и устройство привода самих ног. Машина будет оснащена двумя парами механических ног, которые будут состоять из трех звеньев. На конце нижних звеньев устанавливается платформа, которая непосредственно будет соприкасаться с земной поверхностью. Целесообразно использовать несколько различных платформ для разного типа грунта, а также предусмотреть конструкцию платформ для передвижению по снегу. На втором звене ноги будет размещен независимый колесный привод. Для передвижения на колесном приводе следует предусмотреть возможность подъема крайних звеньев ног, при котором машина будет полностью опускаться на колеса.

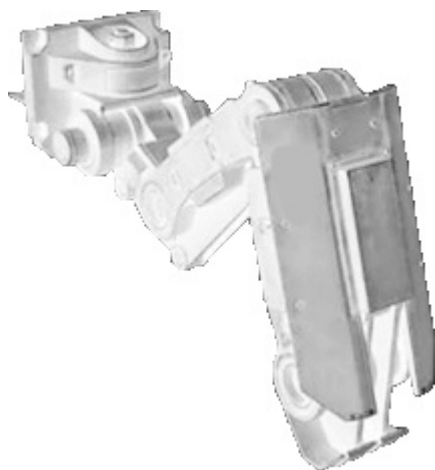


Рис.2.Примерная конструкция механической ноги

Для привода колес возможно использовать различные варианты питания: гидро- или электропривод. Использование гидронасоса с цилиндрическим редуктором логично применять при использовании гидроцилиндров на других механизмах машины (рис. 3) [2].

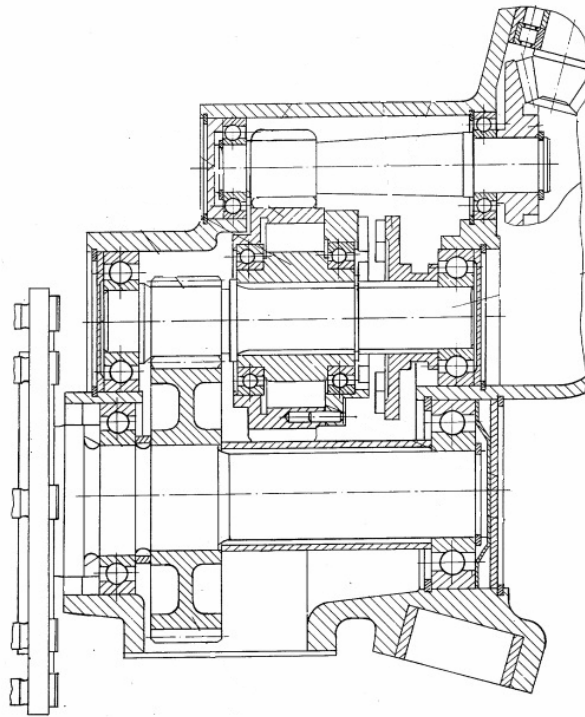


Рис. 3. Цилиндрический редуктор

В качестве привода для колес возможно использовать мотор-редуктор (рис. 4), который потенциально можно будет встроить в диск колеса [3]. Данная конструкция исключит необходимость дополнительного тормоза для колес. При использовании такой схемы возможно применить вместо гидроцилиндров электроцилиндры. Такая конструкция позволяет устранить недостатки «S12 Allroad», но потребует большего количества материальных средств.

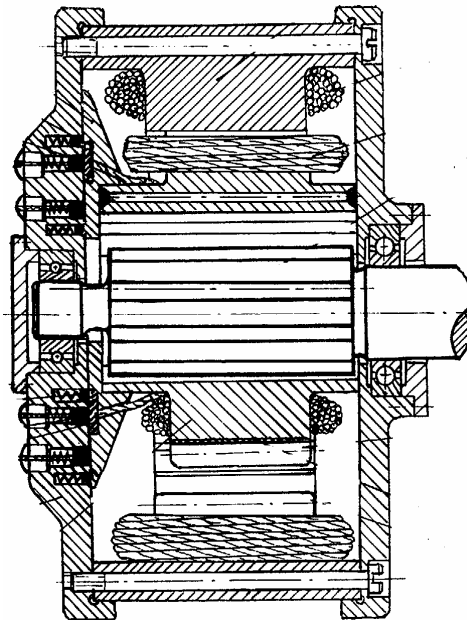


Рис. 4. Планетарный мотор-редуктор

Конструкция машины будет позволять использовать не только стрелу экскаватора, но и различные манипуляторы, что позволит расширить спектр её применения.

Для обеспечения работы машины необходим оператор, который будет непосредственно находиться в кабине или осуществлять управления с пульта на расстоянии.

Создание такого агрегата позволит не только усовершенствовать работу в области ремонтных и монтажных работ, но и откроет дорогу для создания других устройств, основанной на принципе передвижения механических ног.

Список литературы

[1]. [Электронный ресурс] <https://www.kaiser.li/products/new-generation-s10-s12-allroad/> (дата обращения 20.09.2020).

[2]. *Патент СССР № 2147965/27-1, 23.06.1975. Гидравлический индивидуальный привод для управляемых колес транспортного средства // Патент Союза Советских Социалистических республик № 742178. 1980. Бюл. № 23. / Р.Шульцедитер, Б.Хаушильд, К.Олива, Х.Кратцш.*

[3]. *Патент РФ №2005116565/09, 31.05.2005. Планетарный электромотор-редуктор // Патент России № 2294587. 2007. / П. И. Федотов.*

Черенков Александр Григорьевич – студент кафедры «Подъемно-транспортные системы», КФ МГТУ им. Н.Э. Баумана. E-mail: al.cherenkov2013@yandex.ru

СЕКЦИЯ 10.

**МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ
И ФИЗИКО – МАТЕМАТИЧЕСКИЕ ПРОБЛЕМЫ
ПРОЕКТИРОВАНИЯ СЛОЖНЫХ
ТЕХНИЧЕСКИХ СИСТЕМ**

ИСПОЛЬЗОВАНИЕ МЕТОДА АНАЛИЗА СЕТИ ДЛЯ РЕШЕНИЯ ЗАДАЧИ О МНОГОПОЛЮСНОМ МАКСИМАЛЬНОМ ПОТОКЕ

Имеется неориентированная сеть (рис. 1.2), построенная на основе фрагмента карты дорог города Калуги (рис. 1.1), с ограниченными пропускными способностями дуг b_{ij} (автомобилей в час). Требуется найти величины максимальных потоков между p узлами сети A_i , где i – номер узла (пересечения дорог на карте), где $2 \leq p \leq n$.

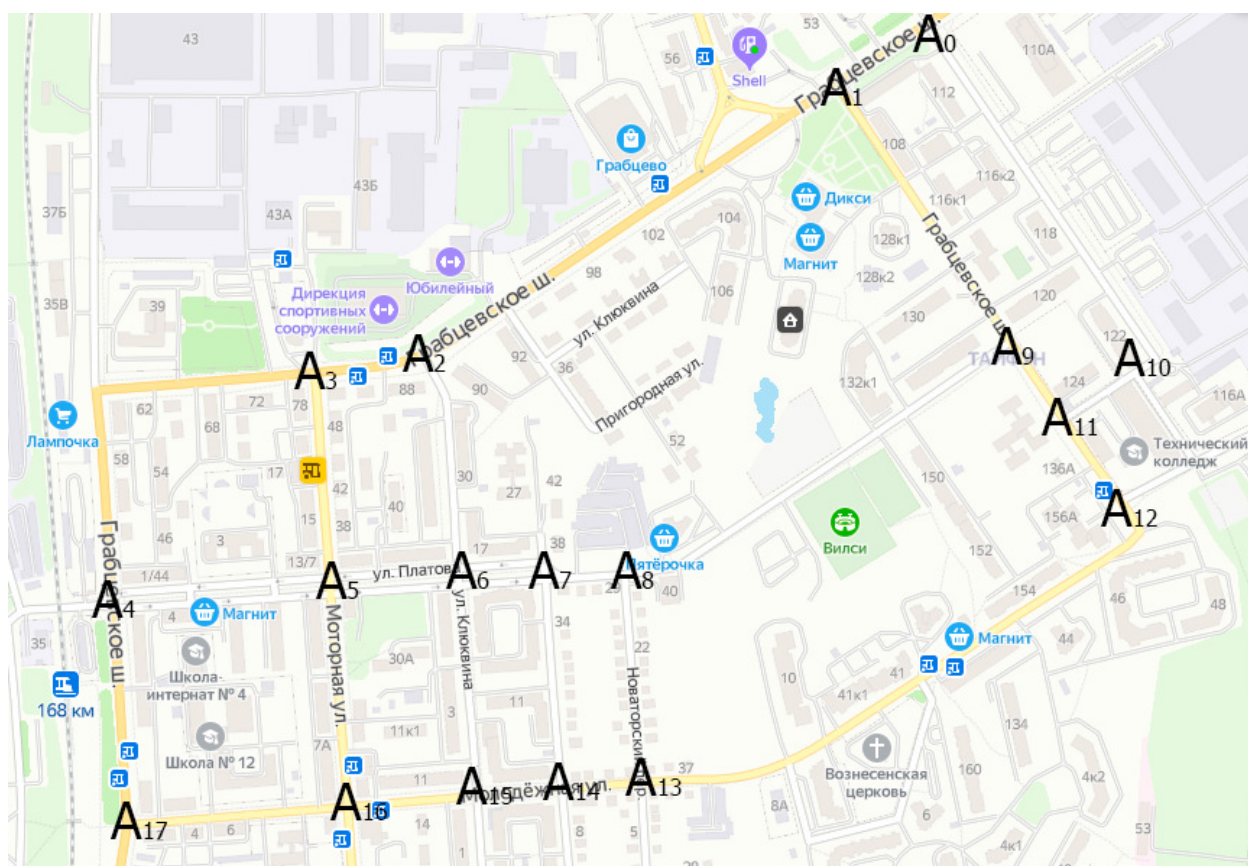


Рис. 1.1. Фрагмент карты дорог

Для решения данной задачи необходимо воспользоваться методом анализа сети. Данный метод позволяет вычислять максимальный поток между p узлами за $p-1$ решений задачи о максимальном потоке, благодаря чему не нужно $\frac{p(p-1)}{2}$ раз вычислять максимальный поток между каждой парой узлов. Причем при решении задачи методом анализа сети каждый раз задача решается в более простой сети, чем исходная.

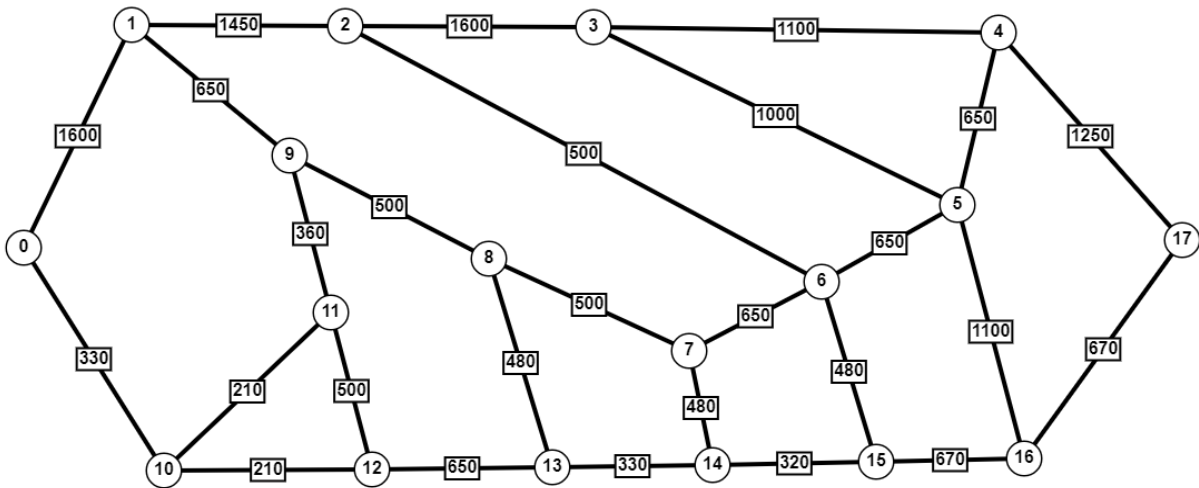


Рис. 1.2 Преобразованная сеть из карты дорог

Метод анализа сети заключается в применении к графу двух рекурсивных шагов:

Шаг 1 заключается в решении задачи о максимальном потоке между двумя wybranными полюсами, причем обычно эта задача решается в сети, меньшей, чем исходная сеть N , так как некоторое множество узлов сжато в один узел. При нахождении максимального потока выделяют минимальный разрез, затем переходят к шагу 2.

Шаг 2 заключается в нахождении очередной дуги дерева, при этом используется выделенный на шаге 1 минимальный разрез. (Алгоритм заканчивается, когда найдено $p - 1$ дуг дерева.) Далее выбирается некоторая новая пара полюсов и осуществляется сжатие некоторых подмножеств узлов исходной сети, в результате чего получается сеть, которая будет использоваться в следующий раз на шаге 1. После этого переходят к шагу 1.

Данный алгоритм позволяет найти дерево минимальных разрезов сети, что позволяет найти максимальный поток между любой парой вершин за один проход.

Применим алгоритм для графа на рис. 1.2.

Ход выполнения алгоритма (см. рис. 1.3):

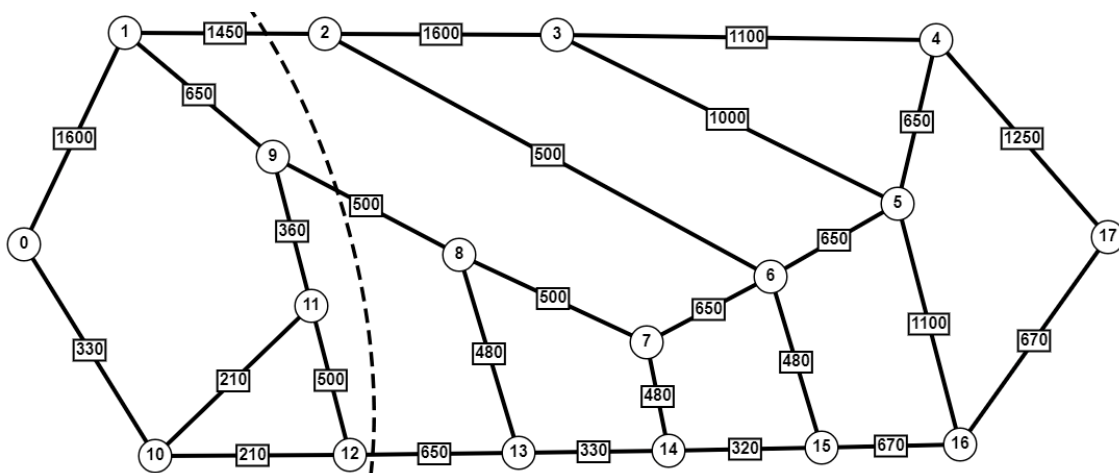


Рис. 1.3. Начальный разрез сети

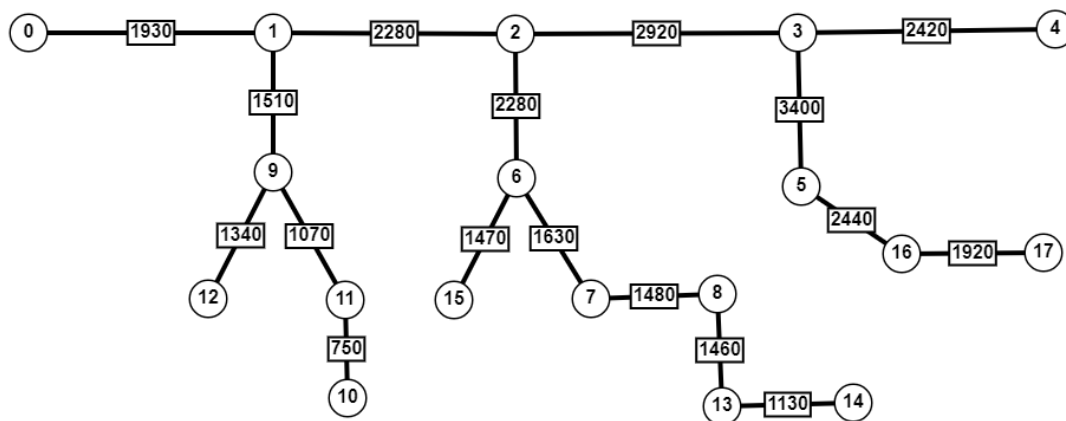


Рис. 1.4. Полученное дерево разрезов

Получив дерево разрезов (рис. 1.4), можно получить таблицу максимальных потоков между любой парой вершин.

Таблица 1.

Результат выполнения метода анализа сети

	A ₀	A ₁	A ₂	A ₃	A ₄	A ₅	A ₆	A ₇	A ₈	A ₉	A ₁₀	A ₁₁	A ₁₂	A ₁₃	A ₁₄	A ₁₅	A ₁₆	A ₁₇
A ₀	∞	1930	1930	1930	1930	1930	1930	1630	1480	1510	750	1070	1340	1460	1130	1470	1930	1920
A ₁		∞	2280	2280	2280	2280	2280	1630	1480	1510	750	1070	1340	1460	1130	1470	2280	1920
A ₂			∞	2920	2420	2920	2280	1630	1480	1510	750	1070	1340	1460	1130	1470	2440	1920
A ₃				∞	2420	3400	2280	1630	1480	1510	750	1070	1340	1460	1130	1470	2440	1920
A ₄					∞	2420	2280	1630	1480	1510	750	1070	1340	1460	1130	1470	2420	1920
A ₅						∞	2280	1630	1480	1510	750	1070	1340	1460	1130	1470	2440	1920
A ₆							∞	1630	1480	1510	750	1070	1340	1460	1130	1470	2280	1920
A ₇								∞	1480	1510	750	1070	1340	1460	1130	1470	1630	1630
A ₈									∞	1480	750	1070	1340	1460	1130	1470	1480	1480
A ₉										∞	750	1070	1340	1460	1130	1470	1510	1510
A ₁₀											∞	750	750	750	750	750	750	750
A ₁₁												∞	1070	1070	1070	1070	1070	1070
A ₁₂													∞	1340	1130	1340	1340	1340
A ₁₃														∞	1130	1460	1460	1460
A ₁₄															∞	1130	1130	1130
A ₁₅																∞	1470	1470
A ₁₆																	∞	1920
A ₁₇																		∞

Таким образом, применяя метод анализа сети, количество вычислений действительно сократилось в $\frac{p-1}{2}$ раз. Данное преимущество будет играть огромную роль при вычислении попарных потоков в больших графах, так как сложность алгоритма метода анализа сети будет на порядок меньше.

Список литературы

[1]. Т. Ху Целочисленное программирование и потоки в сетях. – М.: Изд. Мир, 1974 – 167 с.

Белоножко Павел Евгеньевич – студент КФ МГТУ им. Н.Э. Баумана.
E-mail: belonozhko99@ya.ru

Гагарин Юрий Евгеньевич – канд. техн. наук, заведующий кафедрой
«Программное обеспечение ЭВМ, информационные технологии» КФ МГТУ
им. Н.Э. Баумана. E-mail: Yriigagarin@yandex.ru

ПРИМЕНЕНИЕ МЕТОДА РАССТАНОВКИ ПОМЕТОК ДЛЯ НАХОЖДЕНИЯ МАКСИМАЛЬНОГО ПОТОКА

Метод расстановки пометок начинается с произвольного потока. Затем предпринимается попытка получить поток с большей величиной. Вычисления заканчиваются, когда получен максимальный поток. Алгоритм заключается в систематическом поиске всех возможных путей из N_s в N_t , увеличивающих поток. Это осуществляется с помощью процедуры «расстановки пометок». Узлы получают специальные «пометки», указывающие направление, в котором может быть увеличен некоторый дуговой поток. После того как найден некоторый путь, увеличивающий поток, определяют величину максимальной пропускной способности этого пути; далее поток увеличивают на эту величину, а все пометки на узлах стирают. Затем начинается расстановка новых пометок узлов исходя из только что полученного потока.

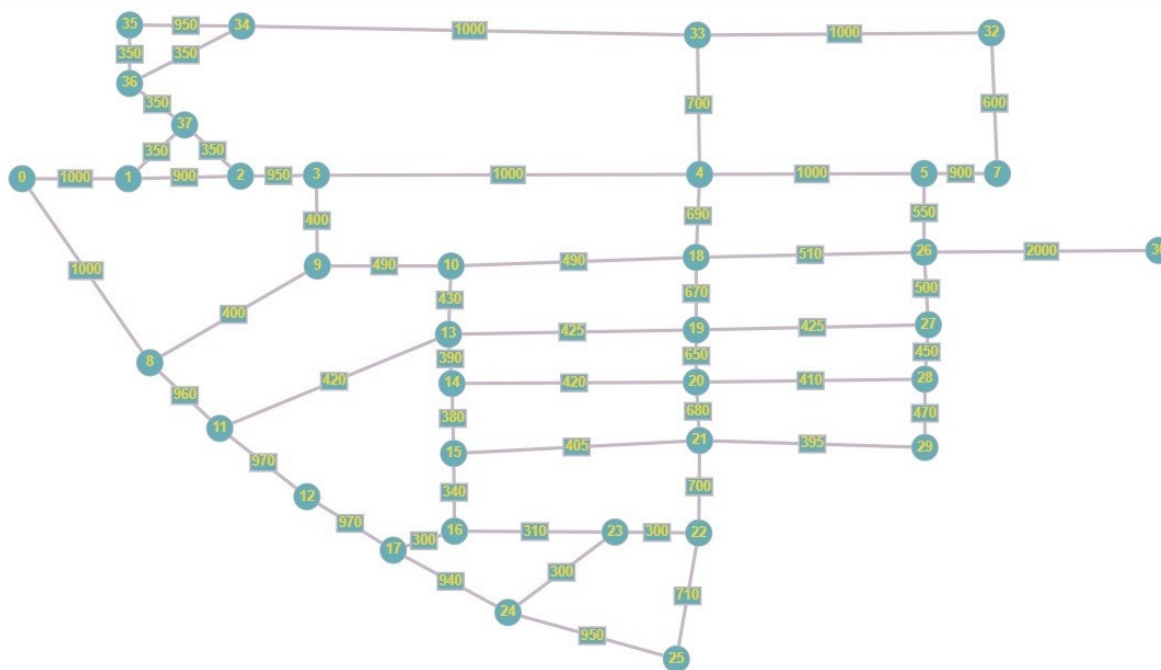


Рис. 1. Фрагмент карты дорог в виде графа

Алгоритм состоит из двух шагов. Шаг 1 – это процесс, в ходе которого узлы получают пометки. Шаг 2 заключается в изменении потока. Шаги 1 и 2 повторяются до тех пор, пока увеличение потока становится невозможным.

Шаг 1 (процесс расстановки пометок). На шаге 1 каждый узел находится в одном из трех состояний: «помечен и просмотрен», «помечен и не просмотрен» или «не помечен». Вначале все узлы не помечены. Пометка произвольного узла N_j всегда состоит из двух частей. Первая часть – индекс i -узла N_i , который указывает, что можно «послать» поток из N_i в N_j . Вторая часть пометки – число, указывающее максимальную величину потока, который

можно «послать» из источника N_s в N_j , не нарушая ограничений на пропускные способности дуг.

Прежде всего источник N_s получает пометку $[s^+, \varepsilon(s) = \infty]$. Первая часть этой пометки означает, что можно послать поток из узла N_s в этот же узел; символ ∞ означает, что величина потока не ограничена сверху. Теперь узел N_s «помечен и не просмотрен», а все остальные узлы «не помечены».

Вообще выберем любой помеченный и непросмотренный узел N_j . Пусть он имеет пометку $[j^+, \varepsilon(j)]$ или $[j^-, \varepsilon(j)]$. Два узла будем называть соседними, если они соединены дугой. Из всех узлов, соседних с N_j , выделим те узлы N_h , которые не помечены и для которых $x_{jh} < b_{jh}$. Припишем каждому узлу N_k пометку $[j^+, \varepsilon(k)]$, где $\varepsilon(k) = \min[\varepsilon(j), b_{jh} - x_{jh}]$. (Такие узлы N_k теперь «помечены и не просмотрены».) После этого всем соседним с N_j узлам N_k , которые не помечены и для которых $x_{hj} > 0$, приписываем пометку $[j^-, \varepsilon(k)]$ где $\varepsilon(k) = \min[\varepsilon(j), b_{jk} - x_{hj}]$. (Такие узлы N_k теперь также «помечены и не просмотрены».) Теперь все узлы, соседние с N_j , имеют пометки. Тогда узел N_j считается помеченным и просмотренным, и его можно больше не рассматривать на этом шаге. Может оказаться, что некоторые соседние с N_j узлы помечены, а остальные не могут быть помечены (либо все соседние с N_j узлы не могут быть помечены); в этих случаях узел N_j также считается помеченным и просмотренным. Знаки «+» и «-» в первой части пометок указывают, как должен быть изменен поток на шаге 2.

Продолжим приписывать пометки узлам, которые являются соседними для помеченных и непросмотренных узлов, до тех пор, пока либо узел N_t окажется помеченным, либо нельзя будет больше пометить ни один узел и сток N_t окажется непомеченным. Если N_t не может быть помечен, то не существует пути из N_s в N_t , увеличивающего поток, и, следовательно, построенный поток максимален. Если же N_t помечен, то на шаге 2 можно найти путь, увеличивающий поток.

Шаг 2 (изменение потока). Предположим, что сток N_t имеет пометку $[t^+, \varepsilon(t)]$. Тогда заменим x_{kt} на $x_{kt} + \varepsilon(t)$. Если же он имеет пометку $[t^-, \varepsilon(t)]$, то x_{tk} заменим на $x_{tk} - \varepsilon(t)$. Затем в любом из этих случаев переходим к узлу N_k . Вообще если узел N_k имеет пометку $[k^+, \varepsilon(k)]$, то x_{jk} заменим на $x_{jk} + \varepsilon(k)$ и перейдем к узлу N_j , если узел N_k имеет пометку $[k^-, \varepsilon(k)]$, то x_{kj} заменим на $x_{kj} - \varepsilon(k)$ и перейдем к N_j . Продолжим эти действия, пока не достигнем источника N_s . После этого сотрем все старые пометки узлов и вновь перейдем к шагу 1.

Чтобы обеспечить конечность процесса, будем предполагать, что дуговые пропускные способности b_{ij} целочисленны. (Ниже будет рассмотрена модификация метода, обеспечивающая конечность процесса при любых неотрицательных b_{ij} .)

Когда алгоритм заканчивается на шаге 1, то получается множество X помеченных узлов и множество дуг A_{ij} с $N_i \in X$, $N_j \in \bar{X}$, на которых $x_{ij} = b_{ij}$ (и пет дуг A_{ji} , таких, что $x_{ji} > 0$). Отсюда следует, что (X, \bar{X}) – минимальный разрез,

поток через который равен его пропускной способности. Таким образом, получен максимальный поток. С другой стороны, каждый раз величина потока увеличивается по крайней мере на единицу (предполагаем, что пропускные способности дуг и исходный поток являются целочисленными). Поскольку величина максимального потока ограничена сверху пропускной способностью минимального разреза (целым числом), то алгоритм расстановки пометок конечен).

```

Консоль отладки Microsoft Visual Studio
Упрощенная матрица пути
0: (0: 9999), (1: 1000), (8: 1000),
1: (0: 1000), (1: 9999), (2: 900), (30: 350),
2: (1: 900), (2: 9999), (3: 950), (30: 350),
3: (2: 950), (3: 9999), (4: 1000), (9: 400),
4: (3: 1000), (4: 9999), (5: 1000), (18: 600), (33: 700),
5: (4: 1000), (5: 9999), (7: 900), (26: 550),
6: (6: 9999),
7: (5: 900), (7: 9999), (32: 600),
8: (0: 1000), (8: 9999), (9: 400), (11: 960),
9: (3: 400), (8: 400), (9: 9999), (10: 490),
10: (9: 490), (10: 9999), (13: 430), (18: 490),
11: (8: 960), (11: 9999), (12: 970), (13: 420),
12: (11: 970), (12: 9999), (17: 970),
13: (10: 430), (11: 420), (13: 9999), (14: 390), (19: 425),
14: (13: 390), (14: 9999), (15: 380), (20: 420),
15: (14: 380), (15: 9999), (16: 340), (21: 405),
16: (15: 340), (16: 9999), (17: 300), (23: 310),
17: (12: 970), (16: 300), (17: 9999), (24: 940),
18: (4: 600), (10: 490), (18: 9999), (19: 670), (26: 510),
19: (13: 425), (18: 670), (19: 9999), (20: 650), (27: 425),
20: (14: 420), (19: 650), (20: 9999), (21: 680), (28: 410),
21: (15: 405), (20: 680), (21: 9999), (22: 700), (29: 395),
22: (21: 700), (22: 9999), (23: 300), (25: 710),
23: (16: 310), (22: 300), (23: 9999), (24: 300),
24: (17: 940), (23: 300), (24: 9999), (25: 950),
25: (22: 710), (24: 950), (25: 9999),
26: (5: 550), (18: 510), (26: 9999), (27: 500), (37: 2000),
27: (19: 425), (26: 500), (27: 9999), (28: 450),
28: (20: 410), (27: 450), (28: 9999), (29: 470),
29: (21: 395), (28: 470), (29: 9999),
30: (1: 350), (2: 350), (30: 9999), (36: 350),
31: (31: 9999),
32: (7: 600), (32: 9999), (33: 1000),
33: (4: 700), (32: 1000), (33: 9999), (34: 1000),
34: (33: 1000), (34: 9999), (35: 950), (36: 350),
35: (34: 950), (35: 9999), (36: 350),
36: (30: 350), (34: 350), (35: 350), (36: 9999),
37: (26: 2000), (37: 9999),
Максимальный поток из 0 в 37 = 1560
C:\Users\Евгений\source\repos\Научка\Debug\Научка.exe (процесс 16212) завершил работу с кодом 0.

```

Рис. 2. Результат работы программы

Вершина 37 в программе соответствует вершине 30 на графе, все остальные вершины на графе и в программе соответствуют друг другу.

Список литературы

[1]. Ху Т. Целочисленное программирование и потоки в сетях. (Integer Programming and Network Flows, 1970) / Перевод с английского П.Л. Бузыцкого, Е.В. Левнера, Б.Г. Литвака. Под редакцией Л.Л. Фридмана. – 1970

Мосин Евгений Дмитриевич – студент КФ МГТУ им. Н.Э. Баумана.
E-mail: lolko40rus@yandex.ru

Гагарин Юрий Евгеньевич – канд. техн. наук, заведующий кафедрой «Программное обеспечение ЭВМ, информационные технологии» КФ МГТУ им. Н.Э. Баумана. E-mail: Yriigagarin@yandex.ru

СЕКЦИЯ 12.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫЕ МАШИНЫ

5G-СВЯЗЬ И ЕЁ ХАРАКТЕРИСТИКА

5G – это новейшее (пятое) поколение технологий мобильной сотовой связи, которое призвано значительно повысить скорость работы интернета, увеличить охват и уменьшить время передачи пакета данных в беспроводных сетях.

Технология 5G придет на смену существующим сейчас 3G и 4G. В 5G собраны все самые последние и совершенные разработки человечества с точки зрения коммуникаций и IT.

Новое поколение мобильной связи 5G, обладает рядом принципиальных преимуществ по сравнению с 4G:

- более высокая скорость передачи данных;
- низкая задержка сигнала;
- возможность подключения большего числа девайсов;
- высокая энергоэффективность;
- многократно возросшая пропускная способность;
- высокая мобильность пользователей.

Ещё одно важное отличие 5G – масштабная виртуализация. Новая технология выходит за рамки одних лишь аппаратных решений. Многие функции в ней реализованы не на уровне физической инфраструктуры, а программным способом [1].

Области применения 5G. Сфера применения 5G довольно широка, начиная от обычного использования смартфона и заканчивая здравоохранением. Также сюда входит концепция умного дома, производственные и вычислительные мощности (IIoT), инфраструктура умного города. Устройства и системы объединяются в общую сеть с дистанционным управлением и контролем при минимальных задержках. В первом случае это могут быть бытовые приборы, климат-контроль, системы экстренного оповещения. Жители городов смогут воспользоваться бесперебойным оперативным доступом к различным сервисам: центрам государственных услуг, городскому транспорту и не только.

Множество видов транспорта может быть переведено на беспилотный режим с целью обеспечения большей точности, надёжности и безопасности процессов. Широко применимыми станут облачные приложения, для которых раньше требовалась установка on-premise. Благодаря скоростной передаче данных пользователи и разработчики смогут совершать операции, требующие высокой аппаратной мощности, имея под рукой только мобильный интернет.

Качественная связь с удалёнными регионами позволит оказывать высококлассную поддержку в случае экстренных ситуаций. Во время сложных операций или диагностики с использованием видеопотока 5G обеспечит высокую скорость и разрешение [2].

В сфере развлечений 5G может использоваться для VR (виртуальной реальности).

Работа 5G. Нередко для сетей нового поколения будет использоваться существующая инфраструктура, доставшаяся в наследство от 4G и более ранних поколений. Благодаря более гибкому кодированию и расширенным каналам передачи данных скорость 5G NR будет на 25-50% превосходить показатели LTE.

Преимущества 5G. Одно из главных достоинств сетей нового поколения – скорость передачи данных. Для рядовых пользователей этот показатель достигнет порядка 10 Гбит/с. Рекордные показатели 5G выдали цифру в 25,3 Гбит/с, в то время как сети LTE едва ли превышают отметку в 100 Мбит/с. Такие скорости позволят смотреть и транслировать видео в 4K и 8K. Фильмы в формате Full HD и должны будут скачиваться в течение минуты. С подобными скоростями сети 5G сделают большой шаг вперед в развитии виртуальной реальности. Для сравнения: сейчас максимальная скорость 4G у абонентов редко превышает 100 Мб/с. Большая пропускная способность сети пригодится для прямых трансляций видео высокой чёткости, работы приложений виртуальной реальности, организации систем удалённого обучения.

Ещё 5G уменьшает задержку сигнала до 1 миллисекунды. Сейчас задержки могут достигать 10 миллисекунд в сетях 4G и 100 миллисекунд в 3G. Улучшение этого показателя позволит использовать мобильное подключение даже в тех ситуациях, когда критически важное значение имеет время отклика. Например, для дистанционного управления сельхозтехникой, промышленными роботами или беспилотными автомобилями. Глобальное распространение сетей пятого поколения приведёт к исчезновению феномена Wi-Fi. Смартфон, планшет или ноутбук всегда и везде будут иметь доступ к интернету, независимо от того, есть рядом роутер или нет.

Опасность 5G. Как и любая новая технология, 5G несёт в себе риски. Оправданы они или нет, сказать трудно – в большинстве случаев мы имеем дело со стадией исследований. Основными угрозами можно считать: кибератаки, пересечение частот и ущерб здоровью.

Интернет вещей подвержен атакам точно так же, как любые электронные устройства. Пользователи должны будут позаботиться об обеспечении безопасности своих девайсов, а компании и государственные органы – предпринять серьёзные усилия для обеспечения защиты умных городов и IoT [3].

Несмотря на планируемый рефарминг, многие спектры частот всё ещё эксплуатируются специальными службами и учреждениями, среди которых научные лаборатории, космические и военные ведомства. Выделение диапазонов для коммерческого использования потребует тщательного всестороннего согласования.

В июле 2019 года ряд российских ведомств заявили, что намерены проанализировать влияние сетей 5G на здоровье населения. Минздрав, Минкомсвязь, Роспотребнадзор, Федеральное медико-биологическое агентство

(ФМБА) и департамент информационных технологий Москвы (ДИТ) проведут исследования и сформулируют актуальные нормативы.

В ходе проведённых опытов было установлено, что новые технологии мобильной связи способны разрушить внутреннюю систему координации животных в пространстве.

Первые жертвы сети 5G уже появились в Голландии: после запуска вышки там в радиусе 400 метров вымерли несколько сотен скворцов. Также странный эффект запуск вышек произвёл на коров: в районе, где проводилось тестовое использование вышек, коровы на фермах начинали впадать в сильное беспокойство, и вышки пришлось отключить. Швейцарская организация ProNature установила, что излучение 5G-вышек повышает температуру тела насекомых. Стоит отметить, что частота, которая соответствует диапазону связи 4G, уже сейчас используется для защиты зерна от вредителей, проще говоря, убивает их. А частота 5G является ещё более губительной.

Частота связи 5G оказывает влияние на потовые протоки и железы человека, принцип действия которых во многом повторяет действие антенн. Физик Пол Бен-Ишай поясняет, что потовые протоки человека работают по принципу спиральных антенн. И когда вместо обычного электромагнитного излучения в тело проникают неестественно короткие электромагнитные импульсы, заряды сами становятся излучателями электромагнитных волн и направляют их глубже в тело.

Частота связи 5-G может влиять на ДНК и ускорять процесс старения организма. К такому выводу пришёл доктор Мартин Полл, которые специализируется в области биохимии и медицины. Также в ходе своих исследований он установил, что электромагнитное поле разрушает мозг и нарушает работу сердца. По его словам импульсное электромагнитное поле, которое свойственно именно 5G, более опасно, чем непрерывное.

Также Мартин Полл говорит о том, что электромагнитные волны глубоко проникают в тело человека, поражая и разрушая его ткани. В этом вопросе он ссылается на профессора Хессинга, исследования которого показывают, что у телят тех коров, которые пасутся непосредственно рядом с вышками-излучателями, уже с первых дней жизни формируется катаракта.

Действие вышек 5G очень похоже по своему принципу на действие так называемых СВЧ-пушек, которые применяют для разгона демонстраций. В обоих случаях целенаправленное излучение способно разогревать тело человека (и любого живого существа в принципе) и негативно влиять на самочувствие.

5G может вызывать мутации, причём такие, которые будут передаваться потомкам тех, кто подвергся излучению. Онколог Леннарт Харделл исследовал воздействие на человека технологии предыдущих поколений мобильной связи и отметил любопытную статистику, что опухоль мозга развивается преимущественно с той стороны, с которой к уху прикладывается телефон.

Любопытно, что страховые компании отказываются страховать ответственность телекоммуникационных корпораций в случае подачи против них ис-

ков о нанесении вреда здоровью по причине использования технологий 5G. Одна из крупнейших страховых компаний составила отчёт, согласно которому есть риски, что 5G может нанести человечеству непоправимый вред.

Внедрение 5G. Процесс внедрения сетей 5G в коммерческую эксплуатацию начался уже с 2019 года, правда, пока покрытие таких сетей весьма скромное. На начало 2020 года, сети 5G запущены в эксплуатацию у 47 операторов в 22 странах мира, а вместе с теми, кто запланировал запуск или ведет тестирование будет 279 операторов в 109 странах [4].

Что касается абонентского оборудования, то в продаже уже имеется множество моделей 5G смартфонов, роутеров и CPE.

Первые пользователи уже оценили значительный рост скорости передачи в режиме 5G. Результаты тестов Qualcomm (май 2019) показывают повышение скорости скачивания у 5G устройств по сравнению с LTE устройствами в 3,3 раза. В будущем этот показатель будет выше за счет более плотного покрытия и перехода от LTE EPC ядра к пакетному 5G ядру сети.

В России «большая четверка» операторов в период с августа по сентябрь 2019 года уже провели первые тесты и запуск пилотных сегментов 5G сетей. По результатам тестов на данном этапе задержки в сети в движении вышли менее 10 мсек, а скорости достигали 2 Гбит/сек на скачивание.

Пилотные зоны 5G можно найти на улицах Москвы (Парк Зарядье, Москва Сити, Воробьевы горы, ВДНХ, Сколково, GMS-Hospital, СК Лужники, ст. м. Горький), Казани, Кронштадта и в лабораториях операторов сотовой связи.

Согласно российской программе «Цифровая экономика», устойчивое покрытие сети 5G должно быть обеспечено к 2024 году во всех крупных городах с населением от 1 миллиона человек. В настоящий момент модель развития российских сетей 5G до конца не определена. Проблема, как и в прочих странах, заключается в выборе радиочастотных полос.

Операторы считают наиболее привлекательным для 5G диапазон 3,4-3,8 ГГц (n78 и n79), однако он занят другими пользователями, в основном, военными и спецслужбами, и требует работы по высвобождению. Больше ясности с частотными диапазонами появится в 4-м квартале 2020 после открытых торгов, на которых Роскомнадзор должен распределить радиочастоты в формате аукциона.

Заключение. Стандарт 5G обещает в корне изменить жизнь человечества, внедрив широкий перечень новых технологий. Благодаря высоким скоростям, пропускной способности и низкому отклику станет доступно много интересных технических нововведений, включая интернет вещей, беспилотные автомобили и прогрессивные шлемы виртуальной реальности[5].

Список литературы

[1] Голиков А. М. Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика. – СПб.: Лань, 2018. – 452 с.

[2] Голованова С.В., Корнеева Д.В., Сидорова Е.Е., Юсупова Г.Ф.. Единый оператор инфраструктуры 5G: количественная оценка влияния на рынки // Экономическая политика. – 2019. – № 4. – С. 166–193.

[3] *Жучков А.А., Ашихина М.П., Боранбаева С.М., Булычева А.С.* Анализ рынка услуг сотовой связи в России // Вестник Орел ГИЭТ. – 2017. – № 2. – С. 136–142.

[4] *Погосян В.М.* Информационные технологии на транспорте. – СПб.: Лань, 2019. – 76 с.

[5] *Хакимов Р.И.* Использование числовых оценок в задаче повышения качества сотовой связи // Вестник Таджикского технического университета им. М.С. Осими/ Паёми Донишгохи техникии Тоҷикистон. – 2014. – № 3(27). – С. 56–60.

Гагарин Юрий Евгеньевич – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: Yriigagarin@yandex.ru

Климушина Дарья Викторовна – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: lovely_jelly@mail.ru

ЮТ И ТУМАННЫЕ ВЫЧИСЛЕНИЯ

По данным центра Statista, к 2020 году в мире будут использоваться 30 миллиардов устройств интернета вещей, а в 2025 году это число увеличится до 75 миллиардов. Все эти устройства будут содержать огромное количество данных, которые необходимо эффективно обрабатывать. В настоящий момент интернет вещей строится, в основном, на основе облачных вычислений, но иногда, одни только облачные системы не могут удовлетворить требований более быстрого анализа и возрастающего объёма данных. Основными недостатками облачных систем при использовании в интернете вещей являются: высокое время ожидания, время простоя, безопасность и личная информация. Поэтому облачные вычисления начинают вытесняться туманными вычислениями, имеющими гораздо больше преимуществ в сфере интернета вещей. Вместе с тем критериев и рекомендаций по выбору между облачными и туманными вычислениями крайне мало.

Туманные вычисления (англ. Fog computing) – один из видов архитектуры вычислений горизонтального типа, используемый для выполнения объемных обработки, вычислений и хранения данных внутри сети облачных сервисов и конечных устройств локально и через Интернет. Данное понятие Флавио Бономи, вице-президент компании Cisco, ввел в техническую литературу в 2011 году [1]. Выбор термина был обусловлен названием имеющейся концепции – «облачные вычисления». [2]. Концепция Fog Computing была предложена как расширение «облака» до границ сети. С технической точки зрения, концепция туманных вычислений тесно связана с облачными дата-центрами, в которых серверы имеют разное местоположение, вплоть до границы сети. Дата-центры могут быть достаточно небольшими (модульного, контейнерного или мобильного исполнения). Таким образом, важной чертой туманных вычислений является близость к конечным пользователям и поддержка их мобильности [3].

Облачные и туманные вычисления имеют схожую базу IT-ресурсов в которую входят вычислительные устройства (как серверы, так и пользовательские процессоры), системы хранения данных и узлы коммутации сети. Но расширение облака до границ сети не ограничивается лишь масштабированием данного облака. Спектр туманных приложений и их техническая реализация могут разительно отличаться от облачных. Однако, данные технологии не являются альтернативами, напротив, они могут плодотворно взаимодействовать, особенно в администрировании и аналитике данных, порождая новый класс приложений. Архитектура Fog Computing представляет собой некую «прослойку» на границе между облаком и устройствами интернета вещей с сенсорами, а также мобильными устройствами пользователей. Основные архитектурные отличия Fog от Cloud:

- Обеспечение качества услуг (QoS, Quality of Service), требующее динамической адаптации приложений к состоянию сети.
- Отслеживание местоположения (Location Awareness) для того, чтобы поддерживать стабильность работы приложения в условиях мобильности терминала.
- Отслеживание контекстной информации (Context Awareness), т.е. определение наличия доступных ресурсов вблизи, чтобы использовать их в работе приложения, с возможностью горизонтального взаимодействия.

В Fog архитектуре сетевые узлы (Fog Sites), расположенные ближе к облачным дата-центрам, обладают наибольшей вычислительной мощностью и большим объемом данных в системах хранения. Сетевые узлы, рядом с сенсорами интернета вещей и мобильными устройствами, обладают быстрым откликом и большей интерактивностью. Отличительной чертой Fog является возможность использовать пользовательские устройства в качестве сетевых узлов. Для этого пользователю необходимо дать разрешение на использование его устройства в фоновом режиме в обмен на разнообразные льготы. Вышеописанные архитектурные особенности обеспечивают следующие преимущества туманных вычислений:

- Снижение нагрузки на облако. Использование туманных технологий совместно с облачными снижает нагрузку на ЦОД. Локальные сервера занимаются обработкой данных и отправляют в дата-центр только самые важные.
- Передача данных в режиме реального времени. «Туман» находится ближе к пользователю, поэтому время на обработку и передачу информации снижается.
- Повышенная безопасность. В локальной сети можно установить дополнительный уровень защиты – например, виртуальный межсетевой экран или сегментацию трафика.

Рекомендации по применению в IoT. В основном, туманные вычисления используются для услуг и приложений, которые имеют плохую работоспособность или не способны работать в архитектуре облачных вычислений. В первую очередь, это сфера интернета вещей, нарастающее развитие которой не может поддерживаться только при помощи облачных решений. Развитие интернета вещей столкнулось с потребностью в фильтрации и предобработке данных перед отправкой в облако. К таким приложениям можно отнести:

- Приложения, требующие низкой и предсказуемой задержки передачи информации по сети.
- Транспортные приложения, такие как: автомобили с беспилотным управлением, скоростные поезда, интеллектуальные транспортные системы и др.
- Приложения, с необходимостью в локальной обработке данных в реальном времени, такие как: интеллектуальные транспортные системы (ИТС), умные системы электроснабжения, управление трубопроводами,

геофизическая разведка недр, сенсорные сети мониторинга окружающей среды и пр. Использование данных приложений требует выполнения вычислений либо в самом источнике информации, либо в устройстве, которое расположено в границах сетей доступа или агрегации [4].

Подход затуманивания имеет много преимуществ для интернета вещей, больших данных и аналитики в реальном времени. Вот основные преимущества туманных вычислений над облачными в сфере интернета вещей:

- низкое время отклика (туман географически ближе к пользователям и способен обеспечить мгновенный отклик);
- отсутствие проблем с пропускной способностью (часть информации агрегируется в разных точках, вместо централизованной отправки по одному каналу);
- невозможность потери соединения (благодаря множеству соединенных каналов);
- высокая безопасность (обработкой данных занимается огромное количество узлов в сложной распределенной системе);
- улучшенный пользовательский интерфейс (мгновенный отклик и отсутствие простоев вызывают положительную реакцию пользователей);
- энергетическая эффективность (в периферийных узлах используются высокоэффективные протоколы, такие как Bluetooth, Zigbee или Z-волна).

Основная цель туманных вычислений – переместить все вычисления как можно ближе к краю сети, уменьшая необходимость удалённых коммуникаций через центральное облако и связанные с этим задержки и перегрузку полосы пропускания ядра сети. В связи с ограничением вместимости и вычислительной мощности из-за использования подключенных устройств интеграция с вычислениями в облаке может обеспечить:

- Улучшение работы (быстрая связь между датчиками IoT и системами обработки данных);
- Вместимость (хорошо масштабируемое и неограниченное место для хранения в состоянии объединить, соединить и распределить огромный объем данных);
- Возможная обработка (удаленные центры обработки данных предоставляют неограниченные виртуальные возможности обработки по требованию);
- Снижение затрат (лицензионные сборы меньше, чем стоимость оборудования на начальном этапе, и его постоянное обслуживание).

С учетом описанных преимуществ, туманные вычисления больше всего подходят для таких сфер как: транспорт, торговля, здравоохранение энергетика, коммунальные службы, сельское хозяйство, а также промышленное производство.

Использование автономными системами управления транспортом (ADS, Autonomous Driving System) различных многорежимных сенсоров, и технологий компьютерного зрения и анализа изображений, спутниковое и сетевое

позиционирование на картах и предиктивную аналитику требует высокого быстродействия, которое может быть обеспечено путем расположения Fog-узла с элементами AI в самом транспортном средстве.

В медицине туманные системы используются, когда нужно предпринять срочные действия в соответствии с планом лечения на основе анализа полученных с датчиков данных. Например, туманные технологии уже используются для контроля состояния больных диабетом и автоматического введения инъекций [5]. При достижении критического значения содержания сахара в крови сенсор на теле пациента выдает сигнал через Fog-сеть на выполнение инъекции при помощи микро-шприца, также расположенного на теле пациента.

Вариантов применения туманных вычислений может быть очень много, и развитие смежных технологий будет добавлять новые сценарии использования. Другие тенденции, в которых так или иначе, использование решения Fog является рациональным, следующие:

- безопасность в интернете вещей;
- блокчейн для интернета вещей;
- использование беспроводных технологий с низкой потребляемой мощностью и высокой дальностью связи;
- растущая роль искусственного интеллекта.

Туманные вычисления – это новый виток развития облачных вычислений, который обеспечивает новые возможности создания интеллектуальных устройств интернета вещей. Данная технология решает ряд самых распространенных проблем облачной технологии, среди которых: высокая задержка в сети, трудности, связанные с подвижностью оконечных точек, потеря связи, высокая стоимость полосы пропускания, непредвиденные сетевые заторы, большая географическая распределенность систем и клиентов. Самый большой потенциал развития технологии Fog computing имеют в следующих отраслях: коммунальные службы, здравоохранение, энергетика, транспорт, сельское хозяйство, торговля, промышленное производство.

Список литературы

[1] *Bonomi F., Milito R., Zhu J., Addepalli S.* Fog computing and its role in the internet of things. – Proceedings of the first edition of the MC. Workshop on Mobile cloud computing. 2012. – P. 13–16.

[2] *Chiang M., Balasubramanian B., Bonomi F.* Fog for 5G and IoT. – Wiley, 2017. 305 p.

[3] *Lopez V., Velasco L.* Elastic Optical Networks: Architectures, Technologies, and Control. – Springer, 2016. – 299 p.

[4] *Шалагинов А.В.* Генезис и будущее облачных вычислений, или досу- жие размышления о «третьем глазе» // ИКС. 2015. – №9–10. – С. 60–63.

[5] *Fog Computing and Edge Computing Architectures for Processing Data From Diabetes Devices Connected to the Medical Internet of Things.* Journal of Diabetes Science and Technology 2017. – Vol. 11(4). –С. 647–652

Тронов Кирилл Александрович – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: Kirtron999@yandex.ru

Красавин Евгений Васильевич – доцент, к.т.н. Калужский филиал МГТУ им. Н.Э. Баумана. E-mail: aleksiis@yandex.ru

АНАЛИЗ АППАРАТНОЙ РЕАЛИЗАЦИИ ОПЕРАЦИИ УМНОЖЕНИЯ КВАТЕРНИОНОВ

Достичь наибольшей скорости вычислений от устройств, которые встраиваются в оборудования систем управления различного направления, можно за счет изменения алгоритма, благодаря которому вычисляются данные для формирования управляющих воздействий, и реализации данного алгоритма на аппаратном уровне. В настоящее время внимание разработчиков систем управления подвижными объектами, привлекают алгоритмы управления на базе кватернионов, которые имеют ряд преимуществ по сравнению с другими способами описания вращательного движения твердого тела.

Кватернион – это упорядоченная четверка действительных чисел, содержащая в себе информацию о скаляре и трехмерном векторе [1].

Кинематические уравнения движения твердого тела в кватернионах не вырождаются, как это имеет место при использовании углов Эйлера, и не содержат тригонометрических функций, а число этих уравнений существенно меньше, чем число уравнений в направляющих косинусах [2].

Для выбора наилучшего варианта для дальнейшей реализации операции умножения кватернионов осуществлен морфологический анализ. Критерием выбора является наименьшее количество операций (и наибольшее быстродействие) при выполнении определенных алгоритмов.

Количество вариантов, исходя из таблицы:

$$3^2 * 4^2 * 6^1 = 864.$$

Форма представления кватерниона. Использование трудоемкой операции извлечения корня из компонент требуется только в случае использования тригонометрической формы представления кватерниона. Исключив данную форму, можно опустить параметр E и избавиться полностью от последней строки табл. 1.

Таким образом, количество вариантов сократится до $2^1 * 4^2 * 6^1 = 192$.

Форма представления компонент кватерниона. Произведем оценку аппаратно-программных ресурсов для выполнения арифметических операций над числами в данных форматах по реализации операции сложения, так как данная операция является наиболее трудоемкой, из-за того что при выполнении данной операции необходимо добиться равенства позиционных весов складываемых (вычитаемых) разрядов.

В форме представления с фиксированной запятой все числа изображаются в виде последовательности цифр с постоянным для всех чисел положением запятой, отделяющей целую часть от дробной [3].

Формальное представление чисел с плавающей запятой в стандарте IEEE 754 для любого формата точности включает в себя бит знака, смещенную экспоненту двоичного числа, остаток мантиссы двоичного нормализованного числа с плавающей точкой.

Морфологическая таблица

Имена признаков/ параметров		Альтернативы					
		1	2	3	4	5	6
А	форма представления кватерниона	полиномиальная	матричная	тригонометрическая			
В	форма представления компонент кватерниона	фикс запятая	плав запятая (короткий формат)	плав запятая (длинный формат)	плав запятая (расширенный формат)		
С	алгоритм сложения компонент	сложение с плавз.	сложение с фикс з. в прямом коде	сложение с фикс з. в обратном коде	сложение с фикс з. в дополнительном коде		
Д	алгоритм умножения компонент	умножение с плав з.	умножение с фикс з., начиная с младших разрядов множителя, в доп. коде	ускоренное умножение с фикс з., алгоритм Лемана в прямом коде	ускоренное умножение с фикс з., алгоритм Мак-Сорлив доп. коде	умн-е с фикс з., начиная с младших разрядов множителя, в прямом коде	умн-е, начиная с младших разрядов множ-ля, со сдвигом суммы частичных произведений в доп. коде
Е	алгоритм извлечения корня из компонента	использование формулы Ньютона	разложение в ряд Маклорена	алгоритм, подобный делению			

Для выполнения операции сложения в формате с фиксированной запятой необходимо выравнивать масштабы слагаемых. Для успешного решения необходимо знать наибольшие значения слагаемых и их суммы. Они аналитически рассчитываются индивидуально для каждой операции, появляющейся в алгоритме, и каждая конкретная операция программируется индивидуально. Вследствие этого разработчик тратит значительное количество времени на подготовку операций, однако выполнение разработанной программы требует минимальных аппаратных и временных затрат.

Для выполнения операции сложения чисел в формате плавающей запятой возможно создание универсального алгоритма для всех операций, появляющихся в некоторой последовательности операций, поэтому разработчик тратит намного меньше времени на подготовку операции. При этом за счет большего количества

операций время выполнения операции намного больше, чем время выполнения операции в формате с фиксированной запятой.

Таким образом, по критерию – быстродействие – можно выбрать формат фиксированной запятой, что сократит количество вариантов до:

$$2^1 * 1 * 3^1 * 5^1 = 30.$$

Форма представления кватерниона. Использование полиномиальной формы при выполнении операции умножения потребует 12 сложений и 16 умножений компонент, а матричная форма – 48 и 64 соответственно. Использование полиномиальной формы является более целесообразным. Таким образом, количество вариантов сократится до $1 * 1 * 3^1 * 5^1 = 15$ согласно табл. 2.

Таблица 2.

Морфологическая таблица (2)

Имена признаков/параметров		Альтернативы					
		1	2	3	4	5	6
A	форма представления кватерниона	полиномиальная					
B	форма представления компонент кватерниона	фикс запятая					
C	алгоритм сложения компонент		сложение с фикс з. в прямом коде	сложение с фикс з. в обратном коде	сложение с фикс з. в дополнительном коде		
D	алгоритм умножения компонент		умножение с фикс з., начиная с младших разрядов множителя, в доп. коде	ускоренное умножение с фикс з., алгоритм Лемана в прямом коде	ускоренное умножение с фикс з., алгоритм Мак-Сорли в доп. коде	умн-е с фикс з., начиная с младших разрядов множителя, в прямом коде	умн-е, начиная с младших разрядов множ-ля, со сдвигом суммы частичных произведений в доп. коде
E							

Алгоритм сложения компонент. Для сложения компонент в дополнительном коде, в отличие от прямого кода, требуется предварительный перевод чисел. Однако в дополнительном коде, в отличие от прямого, сложению подвергаются и цифровые разряды мантииссы, и знаковые. Также в дополнительном коде, в отличие от обратного кода, при возникновении переноса из знакового разряда он отбрасывается, не складывается с младшим разрядом суммы.

Поэтому предпочтительнее выбрать сложение с фиксированной запятой в дополнительном коде.

Алгоритм умножения компонент. Так как для сложения выбран алгоритм для чисел, представленных в дополнительном коде, то для того, чтобы избежать дополнительного перевода, следует выбрать алгоритм умножения в дополнительном коде. Тогда количество вариантов сократится до:

$$1 * 1 * 1 * 3^1 = 3 \text{ согласно табл. 3.}$$

Таблица 3.

Морфологическая таблица (3)

Имена признаков/параметров		Альтернативы					
		1	2	3	4	5	6
А	форма представления кватерниона	полиномиальная					
В	форма представления компонент кватерниона	фикс запятая					
С	алгоритм сложения компонент				сложение с фикс з. в дополнительном коде		
Д	алгоритм умножения компонент		умножение с фикс з., начиная с младших разрядов множителя, в доп. коде		ускоренное умножение с фикс з., алгоритм Мак-Сорли в доп. коде		умн-е, начиная с младших разрядов множ-ля, со сдвигом суммы частичных произведений в доп. коде
Е							

Алгоритм умножения компонент. В качестве алгоритма умножения выбран алгоритм ускоренного умножения Мак-Сорли в дополнительном коде, так как, несмотря на усложнение арифметических и логических схем, он позволяет существенно повысить быстродействие ЭВМ, по сравнению с алгоритмами умножения, начиная с младших разрядов множителя, со сдвигом суммы частичных произведений и без сдвига.

Таким образом, в результате морфологического анализа по таблице 3 выбран следующий вариант:

- А1 – форма представления кватерниона - полиномиальная;
- В1 – форма представления компонент кватерниона – фиксированная запятая;
- С4 – алгоритм сложения компонент – сложение с фиксированной запятой в дополнительном коде;
- Д4 – алгоритм умножения компонент – алгоритм ускоренного умножения Мак-Сорли в дополнительном коде.

Данный выбор осуществлен только по критерию быстродействия вычислений, не учитываются дополнительные аппаратные затраты из-за усложнения арифметических и логических схем.

Список литературы

[1]. *Гордеев В. Н.* Кватернионы и бикватернионы с приложениями в геометрии и механике / В.Н. Гордеев. – Киев: Издательство «Сталь», 2016. – 316 с.

[2]. *Амелькин Н.И.* Кинематика и динамика твердого тела. – М.: МФТИ (ГУ), 2000. – 64 с.

[3]. *Представление чисел в ЭВМ.* – URL: https://studref.com/516523/informatika/predstavlenie_chisel (дата обращения: 02.11.2020).

Булкина Анастасия Михайловна – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: an.bulkina23@gmail.com

Максимов А.В. –

Е.В. Красавин, В.О. Трешневская

ВЫБОР ПЛАТФОРМЫ ДЛЯ ВЕБИНАРОВ В ЛОКАЛЬНЫХ СЕТЯХ: МАСШТАБИРУЕМОСТЬ, ПРОСТОТА, БЕЗОПАСНОСТЬ

Внастоящее время в связи с эпидемиологической ситуацией значительно возросла актуальность различных решений в области проведения видеоконференций и вебинаров [1]. В связи с тем, что аппаратные решения, обладающие высокими потребительскими характеристиками, являются очень дорогими, популярность получили программные решения, которых в настоящее время насчитывается несколько десятков [2].

Таблица 1.

Характеристики наиболее популярных платформ для вебинаров

	Skype	Zoom	Webinar.ru	YouTube	Google Hangouts
Количество участников	50	1000	300	нет ограничения	250
Демонстрация экрана	+	+	+	требуется специальный софт	+
Передача файлов	+	+	+	-	+
Общий чат	+	+	+	-	+
Ограничения бесплатной версии	отсутствие SkypeOut и SkypeIn	длительность до 40 минут	до 10 участников	нет взаимодействия со спикером	до 10 участников
Стоимость платной версии	по минутная тарификация	от 14,99\$ в месяц	От 4796 руб. в месяц	-	от 5,4\$ в месяц за участника

Выбор конкретного решения зависит от множества факторов: требуемая функциональность, пропускная способность сети, количество участников и их уровень владения компьютерной техникой.

На практике нередкой является ситуация, когда на удаленный способ необходимо перевести планерки, оперативные коммуникации по текущим вопросам, краткосрочное обучение и инструктажи на предприятиях и организациях, обладающих следующими особенностями:

- локальная сеть без доступа к сети интернет по экономическим и организационным соображениям, в том числе связанным с информационной безопасностью;
- невозможность установки дополнительного ПО на рабочие станции по технологическим причинам;

- большая доля рабочего персонала, обладающего минимальными знаниями и навыками работы на компьютере;
- ограниченные финансовые ресурсы;
- невысокие требования по возможностям (создать группу/конференцию, добавить людей, один из участников – ведущий – управляет показом презентации или своего рабочего стола, небольшой обмен информацией между всеми участниками группы).

Перечисленные выше платформы используют облачный сервис, требуют подключения участников к интернет с достаточно объемным трафиком. Вызывает тревогу и вопрос безопасности: регулярно появляются сообщения об обнаружении уязвимостей в этом программном обеспечении. Немало важен и тот факт, что переход от видеоконференций на 5-10 человек к широкоформатным мероприятиям, рассчитанным на несколько десятков участников, требует использования платного тарифа.

Набор решений для развертывания вебинаров на базе локальной сети ограничен. Наиболее популярной из них является TrueConf [3]. TrueConf Server – сервер видеоконференций, поддерживающий несколько режимов вещания: видеозвонок 1-на-1, групповая видеоконференция (симметричная или многоточечная видеоконференция), позволяет связать одновременно до 16 участников. В селекторном совещании могут связаться до 250 удаленных пользователей одновременно. Во всех случаях все участники конференции являются полноценными участниками и могут разговаривать друг с другом посредством функции «Трибуна», запросив её у Ведущего. А также им доступны такие средства для совместной работы как чат, обмен файлами, электронная доска для совместной работы над документом, показ презентаций, показ рабочего стола. TrueConf разрабатывается российской компанией, а поэтому учитывает местные реалии. В частности, нетребователен к качеству соединения, в программе заложена динамическая регулировка битрейта.

Недостатком данного решения является необходимость установки клиентского ПО всем участникам мероприятий и ограничение бесплатной версии – максимально 10 участников. Стоимость TrueConf Server для корпоративной локальной сети значительна – от 170 тыс.руб. на год (20 пользователей)

Так как мы пытаемся сэкономить финансовые средства, будем рассматривать бесплатные системы, готовые для внедрения в компаниях. Они базируются на OpenSource-сервере веб-видеоконференции, не требующем для использования клиентского программного обеспечения.

Наиболее простой и достаточно функциональный продукт – BigBlueButton, обеспечивающий многопользовательские аудио- и видеоконференции, чат и обмен личными сообщениями, запись лекций (слайды, аудио и чат) для дальнейшего воспроизведения, предоставление общего доступа к рабочему столу для практического показа работы с приложениями и ОС, загрузку презентации в формате PDF, функции рисования и виртуальную указку. Для подключения к серверу достаточно использовать веб-браузер с поддержкой AdobeFlash. В своей работе ВВВ использует более десятка

OpenSource приложений: FreeSWITCH, nginx, Flash-медиасервер Red5, MySQL, ActiveMQ, Tomcat, Redis, Grails, Xuggler, OpenOffice.org, ImageMagick, SWFTools и другие [4].

BigBlueButton позволяет организовать конференцию нажатием одной кнопки. Именно в простоте преимущество BBB перед более функциональным и оснащенным, а значит, и чуть более сложным OpenMeetings.

Система веб-конференций ApacheOpenMeetings [5] позволяет организовать проведение аудио- и видеосовещаний в многоточечном режиме, когда к серверу подключены десятки человек.

OpenMeetings построен с использованием технологий Java и XML. Также как и в BigBlueButton в проекте ApacheOpenMeetings в качестве сервера потоковой передачи используется Red5 - Flash-сервер с открытым исходным кодом для живых потоковых решений всех видов. Он написан на Java, поддерживает потоковое видео (FLV, F4V, MP4) и аудио (MP3, F4A, M4A), запись клиентских потоков.

В качестве базы данных может быть использована MySQL, PostgreSQL, Oracle, DB2 или ApacheDerby. Соединение с сервером осуществляется по протоколам HTTP (порт 5080), RTMP (порт 1935), RTMPT (порт 8088). Встроенный менеджер создания резервных копий упрощает резервирование и восстановление работоспособности сервера и перенос в другую систему.

Главный плюс — для видеосовещания не требуется установка дополнительного ПО, достаточно веб-браузера с плагином для поддержки технологии Flash. Предусмотрена возможность записи и последующего проигрывания совещаний и экспорта в AVI/FLV-файл, импорт в конференцию документов более чем 20 форматов и изображений. Участники могут скачать загруженный файл и совместно редактировать, вводя текст поверх оригинала, рисовать и помечать интересные места. Сами конференции могут быть открытыми и частными. Поддерживается два режима:

совещание — до 16 участников, каждый может передавать аудио- и видеоданные;

лекции — до 200 участников, передача аудио и видео только у модератора/лектора.

Предусмотрен также обмен текстовыми сообщениями, настройки позволяют создать опрос. Модератор, организующий конференцию, отправляет всем участникам приглашение, содержащее прямую ссылку, он же управляет всеми доступными им возможностями. При подключении выбирается вариант участия (видео + аудио, только видео или аудио, рисунки), разрешение и ускорение.

Пользователи в конференции могут быть в роли выступающего, модератора (по умолчанию получает создатель конференции) и слушателя. Работа виртуального лектора мало отличается от реального: кроме видео, он загружает документы, используя указку, акцентирует внимание на важных моментах, включает аудио выбранного слушателя. Модератор может назначить любого пользователя выступающим, тогда все внимание будет переключено на него.

Интерфейс пользователя позволяет приблизить отдельные фрагменты, чтобы лучше рассмотреть их, привлечь внимание, «подняв руку», общаться в групповом или приватном чате. Поддерживается разрешение 320 × 240, 640 × 480, 1280 × 720. Количество пользователей, которые смогут одновременно общаться на сервере, зависит от мощности оборудования и пропускной способности канала. Отдельный поток требует 30–50 Кб/с. Для подключения клиентов по умолчанию используется стандартный 80-й порт, который не должен быть занят другим приложением. Установку OpenMeetings сложной назвать нельзя, в последующем эксплуатация особых хлопот не вызывает.

Требования к оборудованию невысоки, минимальные – компьютер 2х/4х 2 ГГц (32/64 бит) и 4 Гб ОЗУ. Для организации 100 соединений достаточно компьютера класса Pentium 4 с 2 Гб ОЗУ.

Опыт регулярного использования с 2014 года и несколько сотен проведенных мероприятий показали эффективность ApacheOpenMeetings для проведения корпоративных совещаний и обучающих вебинаров.

Список литературы

[1]. *Видеоконференцсвязь. До и после пандемии*. Обзор CNewsAnalytics – URL: https://www.cnews.ru/reviews/rynok_videokonferentsisvyazi_2020 (дата обращения 29.10.2020).

[2]. *Обзор 9 русскоязычных площадок для проведения вебинаров*. – URL: <https://texterra.ru/blog/obzor-9-russkoyazychnykh-ploshchadok-dlya-provedeniya-vebinarov.html> (дата обращения 29.10.2020).

[3]. *Решение #1 для удаленной работы и видеоконференцсвязи*. – URL: <https://trueconf.ru/> (дата обращения 29.10.2020).

[4]. *BigBlueButton*. – URL: <https://bigbluebutton.org/> (дата обращения 29.10.2020).

[5]. *Инкубатор Apache*. – URL: <http://openmeetings.apache.org> (дата обращения 29.10.2020).

Красавин Евгений Васильевич – доцент, к.т.н. Калужский филиал МГТУ им. Н.Э. Баумана. E-mail: aleksiis@yandex.ru

Трешневская Вероника Октавиановна – доцент, к.т.н. КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: votres@yandex.ru

ИНТЕРНЕТ ВЕЩЕЙ IOT. ПРОТОКОЛЫ

Сегодня Интернет стал всеобъемлющим, затронул почти все уголки земного шара и оказывает немислимое влияние на человеческую жизнь. Однако его путь развития еще не закончился. Сейчас мы вступаем в эру крупномасштабного распространения интернета, когда к сети подключаются тысячи разнообразных устройств. Началась эпоха «Интернета вещей» (сокращенно IoT). Этот термин был определен разными авторами по-разному. Интернет вещей как простое взаимодействие между физическим и цифровым мирами. Цифровой мир взаимодействует с физическим миром, используя множество датчиков и исполнительных механизмов [1]. Другой термин определяет Интернет вещей как парадигму, в которой вычислительные и сетевые возможности встроены в любой объект [2]. Интернет вещей относится к новому виду мира, где почти все устройства и приборы, которые мы используем, подключены к сети. Мы используем их совместно для решения сложных задач, требующих высокой степени интеллекта.

Датчики, исполнительные механизмы, вычислительные серверы и коммуникационные сети образуют основную инфраструктуру Интернета вещей. Однако есть программные аспекты, которые необходимо учитывать. Нам необходимо промежуточное программное обеспечение, которое можно использовать для подключения и управления всеми этими разнородными компонентами. Сегодня область интернета вещей является открытой. Но разработчики сталкиваются с проблемой оптимального выбора инструментов для построения Интернета вещей. Например, при планировании проекта важно учитывать способ подключения устройства и взаимодействия с ним. Для этого мы должны выбрать подходящие протоколы для решения конкретных задач IoT. Кроме этого, для выполнения различных задач необходимо использование различных протоколов. Далее будут рассмотрены наиболее распространенные и перспективные протоколы на сегодняшний день.

Asterisk. Стек различных протоколов Asterisk включает в себя множество функций, доступных в коммерческих системах: голосовая почта, конференц-связь, интерактивное голосовое меню и автоматическое распределение вызовов [3]. Пользователи могут создавать новые функции, путем написания собственных скриптов, используя любой язык программирования, способный работать через стандартные потоки системы. Asterisk позволяет разработчикам создавать телефонные системы или переносить существующие системы.

BACnet (Building Automation and Control Networks). Это стандартный протокол передачи данных, который обеспечивает взаимодействие между различными строительными системами и устройствами в приложениях автоматизации зданий и управления ими [4]. В то время как BACnet не обеспечивает взаимозаменяемость устройств, BACnet предоставляет средства для многих видов базовых и сложных взаимодействий с использованием стандартизиро-

ванных методов, которые доказали свою гибкость и надежность на десятках миллионов устройств.

CAP (Common Alerting Protocol). Основное использование протокола CAP заключается в том, чтобы обеспечить активацию всех видов систем оповещения и оповещения населения. Протокол снижает рабочую нагрузку, связанную с использованием нескольких систем оповещения. Включает повышение технической надежности и эффективности работы [5]. CAP также помогает обеспечить согласованность в информации, передаваемой по нескольким каналам системы. Вторичное применение протокола заключается в нормализации предупреждений от различных источников.

CORBA (Common Object Request Broker Architecture). Протокол для осуществления интеграции изолированных систем. CORBA обеспечивает совместную работу между системами на различных операционных системах, языках программирования и вычислительном оборудовании. CORBA использует объектно-ориентированную модель. Протокол обеспечивает связь между программами, написанными на разных языках и работающими на разных компьютерах.

CWMP (CPE WAN Management Protocol). Это протокол прикладного уровня. Он был создан для удаленного управления оборудованием клиент-помещение (CPE), подключенным к сети интернет-протокол (IP). Протокол управления WAN CPE, предназначен для связи между CPE и сервером автоматической настройки (ACS). CWMP определяет функции: поддержка автоматического конфигурирования, управление образами программного обеспечения, микропрограммное обеспечение, управление программным модулем, управление состоянием и производительностью, диагностика [6]. CWMP – это двунаправленный протокол, обеспечивающий связь между CPE и серверами автоматической конфигурации (ACS). Он включает в себя как безопасную автоматическую конфигурацию, так и контроль других функций управления CPE в рамках интегрированной платформы [7].

DHCP (Dynamic Host Configuration Protocol). Протокол динамической настройки узла (DHCP) предоставляет параметры конфигурации интернет-хост. DHCP состоит из двух компонентов: протокола для доставки специальных параметров конфигурации от DHCP-сервера к хосту и механизма распределения сетевых адресов хостам. DHCP построен на модели клиент-сервер, где назначенные хосты DHCP-серверов выделяют сетевые адреса и передают параметры конфигурации динамически настроенным хостам.

DNP3 (Distributed Network Protocol). Это набор коммуникационных протоколов, используемых между компонентами в системах автоматизации технологических процессов. Его основное применение – коммунальные службы, такие как электрические и водопроводные компании. Использование в других отраслях промышленности не является распространенным явлением.

Ethernet/IP. Промышленный сетевой протокол предоставляет широкий спектр функциональных возможностей. Он имеет ряд достоинств: простота настройки, эксплуатации, обслуживания и масштабирования, совместим со

многими коммутаторами Ethernet. Этот протокол является одним из предпочтительных протоколов для сетевого подключения в корпоративных системах. Он также остается одним из лучших вариантов, когда требуется подключение нескольких устройств, и служит экономичным решением для подключения нескольких компьютеров. Протокол используется в широком спектре устройств, таких как роботы, персональные компьютеры, программируемые логические контроллеры, мэйнфреймы, адаптеры ввода-вывода.

HTTP/HTTPS (Hyper Text Transfer Protocol). Протокол передачи гипертекста. Это протокол прикладного уровня для распределенных, совместных, информационных систем. Универсальный протокол, который может быть использован для различных задач, таких как серверы имен и распределенные системы управления объектами. Особенностью HTTP является типизация и согласование представления данных, что позволяет строить системы независимо от передаваемых данных. Задачи протокола: предоставление доступа к внутренним веб-серверам, находящимся в сетях, защищенных брандмауэрами или NAT, загрузка содержимого веб-страниц в ядро системы, мониторинг работоспособности веб-сервера.

IMAP (Internet Message Access Protocol). IMAP расшифровывается как протокол доступа к интернет-сообщениям. Это способ доступа к электронной почте или сообщениям, которые хранятся на почтовом сервере (возможно, совместно используемом). Другими словами, он позволяет почтовой программе «клиент» получать доступ к удаленным хранилищам сообщений, как если бы они были локальными. Например, электронной почтой, хранящейся на сервере IMAP, можно управлять с домашнего или офисного компьютера, ноутбука во время путешествия, без необходимости передавать сообщения или файлы между этими компьютерами.

LDAP (Lightweight Directory Access Protocol). Протокол прикладного уровня для доступа к службе каталогов, является развитым, гибким и хорошо поддерживает стандартные механизмы взаимодействия с серверами каталогов. Он часто используется для аутентификации и хранения информации о пользователях, группах и приложениях [8]. Сервер каталогов LDAP является довольно универсальным хранилищем данных и может использоваться в самых разнообразных приложениях.

NetFlow. Открытый протокол, встроенный инструмент в программном обеспечении Cisco IOS для характеристики работы сети. Видимость в сети – это незаменимый инструмент для IT-специалистов. IOS NetFlow удовлетворяет различные потребности, создавая среду, где администраторы используют инструменты, чтобы понять, кто, что, когда, где и как использовал сетевой трафик. Данный протокол уменьшает уязвимость сети, и позволяет эффективно работать в ней. Улучшение работы сети снижает затраты и приводит к увеличению доходов бизнеса за счет лучшего использования сетевой инфраструктуры.

Сегодня в сети используются сотни различных протоколов. С внедрением Интернета вещей в нашу жизнь, с ростом многообразия устройств, подключенных к сети, и с расширением спектра возлагаемых на них задач,

количество протоколов будет только увеличиваться. Каждый протокол в архитектуре системы IoT обеспечивает взаимодействие между устройствами, между устройством и шлюзом, между шлюзом и центром обработки данных, а также обмен данными. Данная статья описывает и указывает на особенности применения различных протоколов и технологий для конкретных случаев.

Список литературы

- [1]. *Weyrich M. and Ebert C.* Reference architectures for the internet of things, *IEEE Software*. – 2016. – P. 112-116
- [2]. *Internet of Things: Architectures, Protocols, and Applications*. – URL: <https://www.hindawi.com/journals/jecse/2017/9324035/> (дата обращения: 23.10.2020).
- [3]. *A Simple Explanation Of 'The Internet Of Things*. – URL: <https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#174744551d09> (дата обращения: 25.10.2020).
- [4]. *BACnet* (Building Automation and Control networks). – URL: <https://www.loytec.com/products/functions/bacnet>(дата обращения: 25.10.2020).
- [5]. *M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Cla*, Middleware for internet of things: a survey, *IEEE Internet of Things Journal*, – 2016. – P. 70-95.
- [6]. *Software Technologies for Complex Control Systems*. – URL: <https://www.sciencedirect.com/topics/computer-science/common-object-request-broker-architecture> (дата обращения: 26.10.2020).
- [7]. *CPE Wan Management Protocol (CWMP)*. – URL: <https://documentation.media5corp.com/pages/viewpage.action?pageId=69042254> (дата обращения: 26.10.2020).
- [8]. *Lightweight Directory Access Protocol*. – URL: <https://ldap.com/> (дата обращения: 27.10.2020).

Гаранин Никита Андреевич – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия E-mail: n.garanin2014@yandex.ru

Красавин Евгений Васильевич – доцент, к.т.н., Калужский филиал МГТУ им. Н.Э. Баумана. E-mail: aleksiis@yandex.ru

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОТСЛЕЖИВАНИЯ МЕСТОПОЛОЖЕНИЯ И ИХ ИСПОЛЬЗОВАНИЕ В СИСТЕМЕ «УМНЫЙ ГОРОД»

Для построения системы «Умного города» необходимо учитывать огромное количество различных параметров – имеющиеся и требуемые каналы, виды связи, расстояния между устройствами, требуемая скорость передачи данных и уровень энергопотребления и др. И для каждого сочетания данных требований требуется находить наиболее подходящее решение. Несмотря на то что ряд российских и мировых компаний предлагает готовые решения – датчики, устройства, например [1], и прочую необходимую аппаратуруи ПО для обработки полученных данных, стандартов, единых подходов и рекомендаций, как отмечается в [2], [3] в настоящее время нет или их мало, хотя есть попытки создания стандарта [4]. Это затрудняет выбор наиболее эффективной технологии в каждом случае.

Одним из составных элементов умного города являются технологии отслеживания местоположения с их подсистемами передачи и обработки данных. Они могут быть использованы в различных ситуациях: от системы пропусков и отметок сотрудников на предприятии, остановки автоматических машин при возникновении опасной для приближающихся людей ситуации, контроля позиционирования транспортных средств и др. Для таких систем решающими параметрами являются:

- Охватываемая территория и дальность. На каком пространстве требуется отслеживать местоположение объектов (в пределах города, на территории предприятия, одного помещения);

- Точность определения местоположения. Насколько точно необходимо определять местоположение объекта (несколько метров, несколько сантиметров);

- Скорость передачи данных и частота обновления информации. Насколько часто необходимо проводить отслеживание (ежесекундно, раз в несколько минут, по запросу администратора).

Но на данный момент нет единых канонов использования тех или иных технологий. Поэтому существует проблема, какую именно нужно выбрать, в зависимости от требований и условий их использования. Далее будут рассмотрены различные получившие наибольшее распространение технологии, обеспечивающие необходимый функционал, и предложены рекомендации по их использованию.

Bluetooth. Если требуется только отмечать сам факт присутствия человека (например, на проходной зоне предприятия), то достаточно использовать технологию Bluetooth. Для этого достаточно добавить в пропуск рабочих маячок с поддержкой Bluetooth, а на входе или требуемых переходах установить Bluetooth-приемник с оборудованием передачи данных на сервер. Для подоб-

ных целей разработана специализированная версия технологии с низким энергопотреблением. Когда между приемником и датчиком остаётся несколько метров, они реагируют друг на друга. Остается только фиксировать время срабатывания датчика и передавать полученные данные в центр обработки.

DecaWave. В некоторых ситуациях необходимо отслеживать местоположение объектов с высокой точностью, например, для остановки автоматического транспорта при приближении к людям. Для этих целей рекомендуется технология DecaWave. В нем на объекты, например, на одежде людей также устанавливаются маячки, а отслеживающие датчики устанавливаются на опасное оборудование. Таким образом можно в реальном времени получать сигналы о взаимном положении человека и опасного объекта с точностью до 10 сантиметров. И в случае, если это расстояние оказывается критическим, система соответствующим образом реагирует и отправляет сигнал тревоги персоналу или команду остановки на механизм.

ISO 24730. Если нет жестких требований к отслеживанию местоположение каких-либо объектов в реальном времени, а требуется фиксация лишь раз в несколько минут, то рекомендуется технология ISO 24730. Данный беспроводной протокол работает совместно с протоколом Wi-Fi/802.11, но в промышленных условиях, где усложнена передача РЧ-сигналов ввиду присутствия большого количества металла и прочего оборудования обычно работает лучше. Для организации работы требуется установить несколько датчиков на требуемой площади, а также снарядить необходимые объекты любыми устройствами, способными подключаться к Wi-Fi. Приборы, использующие этот протокол, в условиях прямой видимости могут передавать информацию на расстояния до 1 км. Данная система прекрасно подходит для отслеживания для парковочных пространств, где необходима точность до размера парковочного места.

Ячеистые сети. Существует большое число объектов, на которых важны высокая скорость, низкий уровень энергопотребления, и покрытие большой площади – например, уличное освещение, промышленные здания, офисы. В таких сетях устройства, находящиеся в 10-100 метрах друг от друга, могут обмениваться данными со станцией не напрямую, а через соседние точки. При этом достаточно, чтобы хотя бы одно из них имело связь со станцией, и тогда оно может передавать всю необходимую информацию, а также принимать и распространять смежным устройствам сигналы от базы. Скорость передачи данных при этом достаточно высокая, а при выходе какого-либо устройства из строя, цепочка переконфигурируется автоматически и сеть продолжает работу. Существует множество технологий ячеистых сетей. Одна из наиболее универсальных – 6LowPAN, её чаще всего используют на открытых пространствах, улицах и в зданиях. Другая технология – ZigBee, наоборот, обычно используется с готовыми устройствами для систем умного дома и офиса.

На данный момент существует большое количество различных программных и аппаратных решений, позволяющих отслеживать местоположение

каких-либо объектов, таких как Bluetooth, DecaWave, ISO 24730, ячеистые сети и ряд других. Каждая из рассмотренных технологий уже сейчас широко распространена и применяются в различных сетях. Для решения каждой отдельной проблемы важно детально изучить каждую технологию, понимать принцип работы и возможные области применения.

Список литературы

[1]. *Octavian Adrian Postolache, Edward Sazonov, Subbas Chandra Mukhopadhyay. Sensors in the Age of the Internet of Things: Technologies and applications (Control, Robotics and Sensors).* – Institution of Engineering and Technology, 2019. – 320 с.

[2]. *Germaine Halegoua. Smart Cities.* – MIT Press, 2020 – 248 с.

[3]. *Carol L. Stimmel. Building Smart Cities: Analytics, ICT, and Design Thinking.* – Auerbach Publications, 2015 – 290 с.

[4]. *Информационные технологии УМНЫЙ ГОРОД. Показатели. Предварительный национальный стандарт Российской Федерации* – URL: <https://d-russia.ru/wp-content/uploads/2020/01/smart-city-1st.pdf> (дата обращения: 01.11.2020).

Жидков Кирилл Артурович – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: krovihe@mail.ru

Красавин Евгений Васильевич – доцент, к.т.н., Калужский филиал МГТУ им. Н.Э. Баумана. E-mail: aleksiis@yandex.ru

ИСПОЛЬЗОВАНИЕ СЕТЕЙ ДАЛЬНОГО РАДИУСА ДЕЙСТВИЯ И ЗАЩИТА УЗЛОВ СИСТЕМЫ УМНОГО ГОРОДА

Умный город [1], [2] может насчитывать тысячи устройств, каждое из которых должно отправлять отчет о своем текущем состоянии. Эти данные от множества узлов удобнее хранить и обрабатывать централизованно, что требует наличия серверов и организации каналов обмена данными и шлюзов между ними и узлами умного города.

Однако возникает проблема выбора типа технологий и сетей для передачи данных умных устройств и проблема защиты этих данных. Вместе с тем, в настоящее время отсутствуют какие-либо стандарты в этом направлении, хотя предварительная работа ведется [5]. Для выработки рекомендаций рассмотрим возможные технологии более подробно.

2G (GSM). Эти сети используются умными устройствами для передачи данных, так как способны передавать их на большие расстояния (10-15 км), а также делают это в режиме реального времени. Также их преимуществом является то, что данные передаются по специально выделенным частотам и уже имеется готовая сеть базовых станций. Однако явным недостатком их использования является стоимость большого количества сообщений из-за тарифов сотовых операторов.

3G. Данная сеть изначально создана для передачи большого объема данных в режиме реального времени. Также она обладает высокой скоростью связи, но она больше энергопотребление устройствами и не обладает стабильным покрытием (сеть может быть недоступна в сельской и лесной местности, а также в подвалах и колодцах).

Wi-Fi. Сеть Wi-Fi, также как и 3G, была создана для передачи большого объема данных в режиме реального времени. Также она обладает очень высокой скоростью передачи данных и поддержкой на пользовательских устройствах. Однако дальность передачи данных составляет несколько десятков метров, что не подходит для устройств, расположенных в сельской местности, и отсутствие стандартной поддержки mesh-сетей. К недостаткам можно отнести стоимость устройств и роутеров, а также большое энергопотребление устройства.

Сети дальнего радиуса чаще всего используются для передачи сигнала на большие расстояния. Самые используемые сети в этой категории – LoRaWAN и NB-IoT. Они передают данные на несколько километров при условии, что устройство распознает свой шлюз.

Сети такого типа подходят для случаев, когда необходимо собирать данные с различных удаленных объектов, но могут быть неприменимы, если требуется передавать данные датчикам в реальном времени. Все устройства могут создавать связь только на небольшие промежутки времени согласно

требованию регулятора, поэтому передача и прием сигнала могут иметь задержку – от пары секунд и до нескольких минут (а в некоторых случаях даже часов). Но из-за того, что нет необходимости постоянно поддерживать связь между устройствами, заряд батареи расходуется медленнее, и они могут работать без дополнительной зарядки месяцы, а то и годы.

LoRaWAN хорошо подходит для сельской местности – чаще всего в таком типе местности нет хорошего покрытия от действующих сотовых операторов, и мы не можем использовать их сети для передачи данных. Поэтому необходимо будет установить личную базовую станцию (так называют шлюз в этой сети), которая будет получать данные от устройств по технологии LoRaWAN, преобразовывать и отправлять сигналы на сервер по обычным каналам связи. Обычно базовую станцию и сервер устанавливают в непосредственной близости и соединяют с помощью проводных линий.

Для реализации такого подхода необходимы большие вложения в оборудование, но он может обеспечить передачу данных даже из самых удаленных мест. Но при этом невозможно полностью занять частоту передачи данных: все устройства, использующие протокол LoRaWAN, работают в едином диапазоне частот, поэтому возникает риск взаимных помех. Современный город – это целая среда с огромным количеством всевозможных радиосигналов, помех. Поэтому, несмотря на то, что сети LoRaWAN и сейчас могут использоваться в крупных городах, их постепенно вытесняет другие технологии.

NB-IoT лучше справляется с передачей данных в развитых городах, где уже имеются современные и надёжные средства связи. Это вид связи, рекомендованный операторами «большой четверки». Каждому оператору выделен свой радиочастотный диапазон, вследствие чего вероятность того, что будут создаваться взаимные помехи, крайне мала. Сеть проста в развертывании – для подключения к сети достаточно заключения договора с оператором на использование SIM-карт или сразу готовых устройств.

Недостаток – о сети данного вида на данный момент созданы даже не во всех крупных городах. Чаще всего NB-IoT разворачивается там, где уже создана сеть LTE. Также к недостаткам можно отнести стоимость датчиков и тарифы сотового оператора на передачу данных.

Целый ряд компаний уже предлагает готовые решения сетей для Умного города. Примерами таких решений являются сети от Sigfox, «Стриж» и «Вавиот».

С одной стороны, снимается проблема выбора технологий и проекта такой сети. Но у данного подхода также есть и недостатки: зависимость, в том числе с точки зрения информационной безопасности от компании, которая управляет всеми узлами и уровнями вашего интернета вещей.

Особо остро стоит проблема информационной безопасности.

При передаче данных с помощью любой сети необходима организация защиты данных на каждом из уровней узла: физического объекта, канала обмена данными и программы.

Для защиты самого устройства и шлюза на физическом уровне необходимо ограничить доступ к местам установки устройств от риска несанкционированного доступа посторонними лицами. На уровне передачи данных необходимо шифрование каналов связи устройства и его станции, а также канала связи узла с сервером. На уровне ПО обновления должны быть актуальны и проверяться на подлинность для того, чтобы исключить дистанционную несанкционированную загрузку вредоносного программного кода на устройство.

Для защиты сервера на физическом уровне необходимо предусмотреть ограничение доступа к серверу. На уровне передачи данных необходимо шифрование не только в каналах связи между сервером и шлюзом, а также между сервером и конечными пользователями. Также на сервере необходима защита операционной системы. У платформы обычно есть выход в общий интернет – это веб – или мобильные приложения куда выводятся результаты. С учетом этого необходимо ограничить доступ на управление, сделав его только со стороны локальной сети, исключить видимость из внешней сети элементов системы, административных входов.

Для защиты устройств с установленным программным обеспечением для мониторинга данных на физическом уровне необходима защита от несанкционированного доступа к данным, например путем авторизации, возможно двухфакторной. На уровне передачи данных необходима контентная фильтрация для исключения скачивания подозрительного и вредоносного программного обеспечения. На уровне ПО необходима авторизация, разделение ролей в системе, чтобы простые пользователи не имели право на редактирование данных и внос изменений в систему; необходимо регулярно менять пароль. Также необходимо регулярное проведение аудита пользователей на предмет актуальности для исключения доступа к устройствам посторонних и уволившихся сотрудников.

Несмотря на обилие технологий, наиболее пригодны для применения LaRoWAN и NB-IoT. При этом технология LaRoWAN способна наладить связь даже там, где нет устойчивой и постоянной связи, хотя для этого необходимо сделать крупные вложения в инфраструктуру. NB-IoT позволяет использовать уже готовую инфраструктуру с защищенным каналом связи, но на данный момент такая технология доступна лишь в некоторых крупных городах. Все остальные решения накладывают сильные ограничения на выбор устройств либо делают вас зависимыми от подрядчика. Стабильная и корректная работа узлов умного города невозможна без принятия мер информационной безопасности.

Список литературы

- [1]. *Stamatina Th.* Russia, Panos M. Pardalos. Smart City Networks. Through the Internet of Things. – Springer, 2017. –237с.
- [2]. *Germaine Haleboua.* Smart Cities. – MIT Press, 2020 – 248 с.

[3] *BACnet* (Building Automation and Control networks) – URL: <https://www.loytec.com/products/functions/bacnet> (дата обращения: 25.10.2020).

[4]. *Vincent Mosco*. The Smart City in a Digital World. – Emerald Publishing Limited, 2019. – 225с.

[5]. *Информационные технологии УМНЫЙ ГОРОД*. Показатели. Предварительный национальный стандарт Российской федерации. [Электронный ресурс]. – Режимдоступа: <https://d-russia.ru/wp-content/uploads/2020/01/smart-city-1st.pdf>

Сарычева Юлия Юрьевна – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: yulia.sarycheva99@mail.ru

Красавин Евгений Васильевич – доцент, к.т.н., Калужский филиал МГТУ им. Н.Э. Баумана. E-mail: aleksiis@yandex.ru

Трешневская Вероника Октавиановна – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: votres@yandex.ru

СРАВНЕНИЕ ВИРТУАЛИЗАЦИИ И КОНТЕЙНЕРИЗАЦИИ

В современном мире существует множество приложений, которые выполняют различные функции. Все эти приложения должны быть где-то установлены и ранее всегда устанавливались на виртуальные машины.

Виртуализация – это группа вычислительных ресурсов, таких как CPU, RAM и диск, абстрагированных от аппаратной реализации и обеспечивающие при этом логическую изоляцию друг от друга вычислительных процессов, работающих на одной физической машине. Виртуализация используется для запуска нескольких операционных систем на одном компьютере, при этом каждая операционная система работает со своим набором вычислительных ресурсов [1].

Однако подход к развертыванию через виртуализацию имеет недостатки:

1. Поскольку каждая виртуальная машина включает в себя операционную систему и виртуальную копию всего оборудования, необходимого для операционной системы, виртуальным машинам требуются значительные ресурсы оперативной памяти и процессора;

2. Из-за увеличения количества виртуальных копий и требуемых ресурсов, жизненный цикл разработки программного обеспечения становится более сложным с виртуальными машинами;

3. Перемещение виртуальных машин между общедоступными облаками, частными облаками и традиционными центрами обработки данных может быть сложной задачей.

Данные проблемы могут быть решены с помощью контейнеризации. Контейнеризация – это метод обеспечивающий виртуализацию на уровне операционной системы с помощью пространства пользователя. Ядро полностью обеспечивает полную изоляцию контейнеров, поэтому контейнеры не могут напрямую влиять друг на друга [2].

Главное различие между виртуализацией и контейнеризацией заключается в том, что контейнеры разделяют ядро хоста с другими контейнерами. Так же в следствие этого появляется ограничение, из-за которого контейнеры могут быть запущены только с тем же ядром, что и у хостовой системы.

Существует множество реализаций контейнеризации, одной из которых является Docker. Docker – это платформа с открытым исходным кодом, предназначенная для разработки, доставки и запуска приложений. Docker был разработан для:

1. Ускорения процесса разработки приложения;
2. Быстрого тестирования приложения;
3. Быстрого развертывания приложения в production средах;
4. Единообразия сред, в которых будет запускаться приложение.

Приложение Docker состоит из двух компонентов: docker-клиент и docker-daemon. Docker-клиент – это приложение, которое общается с API Docker.

Dockerdaemon – это сервис запускаемый на хост-машине, и который отвечает за всю работу связанную с контейнерами.

Так же Docker включает ряд следующих концептуальных компонентов:

1. Образы – это readonly шаблоны файловой системы, на основе которых создаются контейнеры. Образы состоят из слоев, которые представляют файловую систему со своими файлами на текущем слое, при создании образа используется unionfilesystem, которая объединяет все слои в один готовый образ, что так же позволяет уменьшить его размер.

2. Контейнеры – приложения, запущенные на основе образа. При запуске контейнера, Docker создает readwritеслой поверх существующего образа, что позволяет работать с файловой системой и при необходимости создать на основе контейнера новый образ

3. Реестр образов – хранилище, куда загружаются и откуда скачиваются образы. В реестре образы хранятся в виде слоёв, что позволяет экономить место, потому что часто слои в разных образах повторяются [3].

В результате изучения данной темы можно сделать следующий вывод, что контейнеризация является более предпочтительной технологией для развертывания приложения. Тем не менее, оба способа применяются в современном мире и имеет свои преимущества и недостатки.

Список литературы

[1]. *Виртуализация*. – URL: <https://ru.wikipedia.org/wiki/Виртуализация> (дата обращения 15.10.2020).

[2]. *Контейнеризация*. – URL: <https://ru.wikipedia.org/wiki/Контейнеризация> (дата обращения 15.10.2020).

[3]. *Adrian Mouat. Using Docker 2016*. [Электронный ресурс] Режим доступа: https://store.dockerme.ir/E-Book/Using_Docker.pdf.

Дунаев Александр Владимирович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: sanchezz41@mail.ru

Сергеев Вадим Владимирович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: sergeevvadimlol@yandex.ru

ОБЗОР ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ, ПРЕИМУЩЕСТВ И НЕДОСТАТКОВ СЕРВИСОВ ПО ПРОДАЖЕ И ДОСТАВКЕ ПИЦЦЫ

Пицца – это одно из тех блюд, которое пользуется популярностью и спросом в скромных закусочных и дорогих ресторанах, также есть огромное множество желающих заказать пиццу на дом.

Доставка пиццы – услуга, при которой заказчику доставляют пиццу по указанному им адресу. Заказ пиццы, как правило, предполагает звонок в пиццерию или оформление заказа на сайте.

Всем заведениям, в которых готовят пиццу требуется сайт для автоматизации приемов заказов и отправки по адресу клиента, это облегчит и ускорит работу любой организации. Основным языком является JavaScript, один из самых используемых языков программирования для сайта-строения.

За основу бэкенда мы возьмем `node.js`, современную и удобную платформу. С её помощью мы можем писать системы запросов и ответов для клиента, базы данных и самый тяжелый функционал, который должен на себя брать сервер [1].

В начале проекта он будет без базы данных (БД) и реализация будет на основе фейк сервера, с использованием библиотеки `json-server`. Благодаря данной технологии существует возможность делать тесты с запросами и оптимизацией в самом начале разных проектов. Имитация сервера будет отвечать на запросы с клиента, опраывать все данные связанные с пиццей (название, фото, доступные размеры и тип теста) на главную страницу.

Express создаст основу сервера и с его помощью напишем надежный API (application programming interface).

Позже добавляя БД, используем библиотеку `MongoDB`, она хорошо подходит как для хранения данных пиццы, так и хранения данных пользователей для авторизации и тд. С помощью роутов (логических маршрутов) опишем логику приложения.

Фронтендовскую часть напишем на `react.js`, оптимизированное одностраничное приложение полностью подходит для наших задач. Клиент будет выводить все имеющиеся пиццы на сервере.

Выбираем `react` для сервера из-за этого:

1. Всегда можно сказать, как ваш компонент будет отрисован, взглянув на код.

2. Связывание JavaScript и HTML в JSX делает компоненты простыми для понимания.

3. Можно рендерить React на сервере без перезагрузки страницы.

Мы могли бы использовать `angular`, фреймворк от Google, но он больше подходит для огромных Enterprise проектов. Есть еще вариант с `Vue`, у него достаточно легкий порог вхождения, немного легче чем у `React`, но исходя из

популярности React, у Vue будет меньше так называемая помощь комьюнити. Для нашего фреймворка есть попросту больше написанных библиотек и больше заданных вопросов и ответов на них в [stackoverflow](#).

Приложение должно будет фильтровать и сортировать контент состоящий из пицц. Реализуем это при помощи хуков react. Хуки – конструкции, которые позволяют использовать состояние и другие возможности React без написания классов.

Хуки – это есть простые функции, но для правильного их применения есть несколько правил:

- Использовать их только на верхнем уровне.
- Вызывать хуки только из компонентов React.
- Вызывать из пользовательского хука.

Благодаря этим правилам все состояния будут понятны читающим ваш код. Для соблюдения правил есть хороший плагин для ESLint под названием «[eslint-plugin-react-hooks](#)», принуждающий работать по правилам. Он по умолчанию включен в CreateReactApp.

Хуки решают множество проблем, казалось бы, несвязанных между собой. Добиваясь хорошей производительности обернем компоненты сортировки и фильтра в хук **useMemo**, оборачивая в который мы уберем бесполезный рендер компонентов в ненужный момент, что оптимизирует клиент.

Хук состояния **useState**. Для обновления элемента на странице потребуется использовать **useState**. Он вернет значение с состоянием и функцию для его обновления.

Хук эффекта **useEffect**. Он может выполнять ту же роль, что и `componentDidMount`, `componentDidUpdate` и `componentWillUnmount`, объединяя их в один API.

UseDebugValue может использоваться для отображения метки для пользовательских хуков в ReactDevTools.

UseReducer делает возможным управление внутренним состоянием более сложного компонента с помощью редюсера.

С помощью **useContext**, подписываемся на контекст React без использования каких-либо вложений [2].

Есть другие хуки, которые помогают решать более сложные задачи, а также имеется возможность создавать собственные хуки.

Задействуем TypeScript–улучшенную версию JavaScript, которая была создана для объявления строгой типизации и отлавливания большей части багов во время стадии разработки. С его помощью укажем какие типы обязаны получать наши компоненты.

Для добавления товаров в корзину нам потребуются знания **redux**. Redux – библиотека с простым API предназначенная для управления состояниями приложения в разных компонентах. Redux можно использовать как в Redux, Angular, Vue, так и в других фреймворках, конструируется в основном в кли-

енте. Включает в себя инструменты, которые упрощают передачу данных хранилища через контекст.

При долгих запросах на сервер нам нужно что-то выводить на экран, когда сервер долго отвечает и клиенту нечего грузить, нам поможет библиотека «react-content-loader», которая будет создавать имитацию подгрузки контента как например у Додо-пицца [3].

Для удобства клиента и ввода его данных будем использовать стандартные input для ввода ФИО, номера и т.д., а для указания его местоположения воспользуемся библиотекой «react-yandex-maps», к сожалению библиотека не обладает полной мощностью, как например через CDN. На карте клиент сможет указывать место доставки. С помощью js рассчитаем расстояние от пиццерии до точки заказа.

Платежный модуль напишем с помощью импортирования библиотеки fondy, так клиент сможет выбирать как ему удобнее оплатить онлайн покупку.

Список литературы

[1]. [Электронный ресурс]. – Режим доступа: URL: <https://nodejs.org/en/docs/> (дата обращения 26.10.2020)

[2]. [Электронный ресурс]. – Режим доступа: URL: <https://ru.reactjs.org/> (дата обращения 27.10.2020)

[3]. [Электронный ресурс]. – Режим доступа: URL: <https://www.npmjs.com/package/react-loader> (дата обращения 28.10.2020)

Зейкан Михаил Викторович – E-mail: zeykan_12@mail.ru
Гуркина Е.Д.–

ОБОСНОВАНИЕ ВЫБОРА ИНСТРУМЕНТОВ И ТЕХНОЛОГИЙ АРМ ПРИ ПРОЕКТИРОВАНИИ ПРИЛОЖЕНИЯ ДЛЯ ВОСПИТАТЕЛЯ ДЕТСКОГО САДА

С развитием информационных технологий все больше отраслей нашей жизни переходят в цифровое пространство. Медицина, образование и банковская система уже активно используют информационные технологии. Но в то же время сегодня на рынке программного обеспечения существует мало инструментов для ведения работы воспитателей детского сада.

В своей работе воспитатель сталкивается не только с непосредственным воспитанием детей, но и с заполнением документации, составлением тематических планов, конспектов занятий, составлением распорядка дня и предоставлением информации для родителей. Чтобы облегчить работу воспитателя может быть использовано автоматизированное рабочее место.

Такая система помогает воспитателю оперативно сообщать родителям о случаях плохого поведения ребенка, проводить собрания для родителей (которые не всегда могут присутствовать для этого в детском саду), подготавливать мероприятия для детей, а также составлять отчеты и посещать вебинары для повышения уровня знаний воспитателя.

Автоматизированные рабочие места могут разрабатываться с использованием различных технологий. Выбор наиболее подходящей технологии и является одной из главных задач разработчика.

Разберем данные инструменты подробнее.

Xamarin. Это особый инструмент для создания приложений для всех мобильных платформ, использующий единый язык C#. Xamarin позволяет делать нативные сборки под целевые платформы и создавать высокопроизводительные приложения с естественным внешним видом.

Существует несколько веских причин, по которым Xamarin используется многими компаниями: он использует единый стек технологий для всех платформ, позволяя использовать C# и .NET, а также кроссплатформенные инструменты без дополнительных затрат; предоставляет полный пакет инструментов для разработки, таких как IDE, SDK и инструменты тестирования и аналитики; позволяет устранить все проблемы в совместимости оборудования, используя множество плагинов и API [1].

Однако в использовании Xamarin возникает ряд недостатков, которые особенно сильно заметны при разработке АРМ для воспитателя детского сада. Задержки с обновлениями платформ могут достигать нескольких дней, что фатально скажется на работе приложения. Так же приложение на Xamarin имеет большой размер, что не всегда подойдет для телефонов пользователей. При интеграции сторонних ресурсов с Xamarin могут возникнуть сложности, если необходима будет функция, не представляющая собой платформу [2].

Java. Одной из возможных средств разработки является Java для андроид-приложений. Разработка с помощью данного языка имеет свои плюсы. Оно идеально для тех, кто любит чётко структурировать и разграничивать данные. Также Java имеет большое сообщество и огромное количество уже написанного кода, что существенно облегчает разработку. Работает на огромном количестве ОС с разной конфигурацией аппаратной части. Достигается это благодаря виртуальной машине Java [3].

Однако, виртуальная машина влечет за собой и свои минусы. Низкая скорость выполнения приложения, что критически важно для конечного пользователя АРМ, так как программа должна открываться на любом удобном пользователю устройстве. Также в Java получается громоздкий код, который будет неудобно поддерживать при переходе его к другому разработчику, отсюда следуют высокие требования к написанию рекомендации [4].

Веб-приложение на C#. C# это объектно-ориентированный язык программирования, который обладает сходными с Java плюсами, но лишен критических минусов. Являясь компилируемым языком, C# имеет недостаток в самом процессе компиляции на конкретной машине, однако веб-приложение лишено этого недостатка, так как запускается на заранее выбранном сервере.

Значительным плюсом веб-приложения является доступность его на различных устройствах с доступом в интернет. Для системы АРМ доступ из любого места является отличным аргументом в выборе АРМ пользователем [5].

Также веб-приложение на C# не потребует сложного процесса внедрения, а процесс поддержки и обновления приложения будет зависеть напрямую от разработчика, а не от особенностей устройства пользователя.

Изучив плюсы и минусы существующих АРМ, а также особенности различных средств разработки, можно переходить к обоснованию выбора средств разработки АРМ [6].

Для удобства восприятия информации результаты исследования записаны в табл. 1.

Таблица 1.

Сравнение технологий разработки АРМ

+/-	Быстродействие	Мультиплатформенность	Удобство в эксплуатации	Удобство в поддержке
Xamarin	+	+	-	-
Java	-	+	-	-
Веб-приложение	+	+	+	+

Табл. 1 помогает наглядно определить, какое средство является наиболее приоритетной при разработке АРМ/АИС.

Разработка веб-приложения совмещает в себе все плюсы как разработки на Xamarin, так и на Java, предоставляя большой инструментарий языка C# и .NET, поддерживая как мультиплатформенную составляющую (открытие

веб-приложения осуществляется с помощью браузера, установленного на устройстве), так и предоставляя разработчику удобные инструменты поддержки приложения (изменения в приложение вводятся сразу после внесения их на сервер).

Таким образом, веб-приложение является одним из лучших выборов при разработке АРМ/АИС.

Список литературы

[1]. *Плюсы* и минусы разработки на Xamarin/ [Электронный ресурс]. – Режим доступа: URL: <https://habr.com/ru/post/343098/> (дата обращения: 5.10.2020)

[2]. *Достоинства* и недостатки Xamarin / [Электронный ресурс]. – Режим доступа: URL: <https://habr.com/ru/company/microsoft/blog/415833/> (дата обращения: 5.10.2020)

[3]. *Java vs Kotlin* для Android-разработки: 16 ответов «за» и «против»/[Электронный ресурс]. – Режим доступа: URL: <https://tproger.ru/articles/java-vs-kotlin/> (дата обращения: 9.10.2020)

[4]. *Что* такое Java и зачем он нужен/ [Электронный ресурс]. – Режим доступа: URL: <https://thecode.media/java/> (дата обращения: 9.10.2020)

[5]. *C#* – Преимущества и недостатки / [Электронный ресурс]. – Режим доступа: URL: <https://shwanoff.ru/plus-minus-c-sharp/> (дата обращения: 15.10.2020)

[6]. *Плюсы* и минусы нативных и web приложений / [Электронный ресурс]. – Режим доступа: URL: <http://www.mobilab.ru/articles/nativeorweb.html> (дата обращения: 15.10.2020)

Рязанцев Антон Сергеевич – студент E-mail:
ryazantzev.toscha@yandex.ru
Гуркина Е.Д. –

ОБОСНОВАНИЯ ВЫБОРА ИНСТРУМЕНТОВ И ТЕХНОЛОГИЙ РАЗРАБОТКИ СЕРВЕРНЫХ ЧАСТЕЙ ИГРОВЫХ ПРИЛОЖЕНИЙ

С развитием сферы цифровых развлечений, к которым относят игры, фильмы, музыку и т.д. всё чаще встречается аббревиатура ММО (Массовая многопользовательская онлайн-игра). Являясь наиболее желанным для издателя жанром игр, ММО также являются сложными для реализации проектами, требующими не только слаженной команды разработки, но и выбора непосредственно инструментов разработки. ММО – это онлайн игра, в которой в одном игровом мире/карте присутствует одновременно множество игроков. «Мир» игры располагается на удаленном сервере, либо на кластере серверов, имеющих общую базу данных.

В своей работе разработчик сталкивается с задачами выбора наиболее удобных и уместных для конкретного проекта средств разработки. Однако большой их выбор может ввести в заблуждение и привести к полной отмене проекта, либо к необходимости переписывания исходников под другую технологию.

Если на заре ММО игр разработчикам приходилось разрабатывать свои решения на каком-либо языке программирования, то сейчас существуют и готовые средства разработки, которые не только облегчают настройку проекта, но и позволяют с легкостью обновлять и поддерживать проект [1].

ММО могут разрабатываться на основе разных жанров игр. Часто от жанра и зависит выбор наиболее подходящей технологии разработки. Этот выбор является одной из главных задач разработчика.

Прежде чем изучать инструменты и технологии разработки серверных частей игровых приложений, необходимо определить ключевые понятия данной работы.

Прежде чем рассказывать о предпосылках выбора программных средств для реализации АРМ, необходимо сравнить уже имеющиеся аналоги, учитывая их стоимость, гибкость системы и предоставляемые функции.

Node.js. Node.js – программная платформа, транслирующая JavaScript в машинный код. Позволяет взаимодействовать с устройствами ввода-вывода через API. Вокруг Node.js построено большое сообщество, размер которого растет с каждым днем. Это означает наличие множества фреймворков, а также форумов разработчиков, где каждый может найти решение интересующих его задач [2].

Данный подход хорошо зарекомендовал себя в создании веб-приложений, предоставляя универсальность используемого кода, а также его повторное использование. Минусы технологии могут быть нейтрализованы использованием сторонних библиотек.

Однако, данная технология печально известна сложностью отладки, что требует от разработчика четкого понимания работы своего проекта. В Node.js

не много встроенных средств для упрощения создания серверной части приложения. Разработчик должен иметь достаточно опыта в реализации приложений с использованием Node.js.

Python+Twisted. Twisted – это основанная на событиях среда сетевого программирования, написанная на Python. Проекты на Twisted поддерживают различные протоколы, такие как TCP, UDP, SSL / TLS, IP Multicast, HTTP, XMPP, NNTP, IMAP, SSH, IRC, FTP доменные сокеты Unix [3].

Асинхронные библиотеки программирования, к которым относится Twisted, несомненно, хороши в обработке большого количества операций ввода-вывода параллельно, что играет важную роль при подключении большого числа клиентов.

Однако, использование данного подхода дает большую нагрузку на CPU сервера, что не всегда может продуктивно использоваться в MMO серверах. Также, пока CPU выполняет работу, цикл событий будет заблокирован, что повлечет задержки в действиях большого числа клиентов [4].

Асинхронный код гораздо сложнее понять, чем потоковый. Из этого возникает не только большая ответственность, возложенная на программиста, но и высокие требования к опыту разработчика [5].

Если же команда состоит из разработчиков-новичков, то данный подход приведет к лишним тратам на развертывание большого количества серверов и отладку их работы в кластере с общей базой данных пользователей [6].

Open World Server. При разработке MMO, вполне закономерно ожидать, что в игре должен быть большой бесшовный открытый мир с огромными пространствами, заполненными различными опасностями, монстрами, предметами и активностями. В данном случае особенно хорошо проявит себя бесплатный плагин OpenWorldServer (OWS).

Данная технология разработана на языке C++, который является основным инструментом при разработке игр на движке UnrealEngine (UE). UE – один из самых популярных движков для создания больших и красивых игр. Он имеет не только удобный инструментарий, но и большое сообщество с магазином как бесплатных, так и платных решений, разработанных для игр различных жанров.

OWS – это диспетчер экземпляров сервера, позволяющий создавать большие миры в UE. Поддержка множества карт и большого количества одновременных игроков – всё это есть в OWS. Также OWS позволяет настраивать аккаунты, персонажей, навыки и инвентарь игроков, сохранять их позицию в динамическом игровом мире, настраивать расположение монстров на карте, отслеживать и управлять изменением данных на сервере. В данном плагине также реализовано простое ведение игрового чата, разбитого по каналам.

Однако данная технология имеет значительный минус в зависимости от движка UE. Что требует от разработчика знание C++ и понимания инструментария разработки игрового движка.

Изучив плюсы и минусы существующих инструментов разработки серверных частей игровых приложений, можно переходить к обоснованию выбора технологий разработки.

Для удобства восприятия все плюсы и минусы занесены в Таблицу 1.

Таблица 1.

Сравнение инструментов разработки по критериям

+/-	Node.js	Python+Twisted	Open World Server
Многопоточность	-	+	+
Быстродействие	+	-	-
Удобство поддержки	+	+	+
Менеджер наполнения игрового мира	-	-	+
Менеджер игровых ресурсов	-	-	+
Стоимость разработки (+ если высокая, - если низкая)	+	-	+
Требования к опыту разработчика	+	-	+
Необходимость использования определенного, типизированного игрового движка	-	-	+

На основе табл. 1 четко прослеживается, что выбор UE в совокупности с OWS является наиболее оптимальным для создания MMO проектов. Хотя при использовании данной технологии остается необходимость разработки игры на определенном движке, данный недостаток определенно точно покрывается низкой стоимостью разработки, а также удобством настройки и поддержки игрового мира.

Подход разработки с помощью OWS зарекомендовал себя у небольших команд независимых разработчиков, о чем свидетельствуют упоминания OWS в сообщениях на форумах и в чатах.

Однако при разработке проектов под крылом большого издателя лучшим подходом будет использование независимой технологии, специально разработанной для конкретного проекта.

Список литературы

[1]. *Разработка серверной части многопользовательской онлайн-игры* / [Электронный ресурс]. – Режим доступа: <https://coderoad.ru/30274274/Разработка-серверной-части-многопользовательской-онлайн-игры> (дата обращения: 09.10.20)

[2]. *На чем писать сервер для игры* / [Электронный ресурс]. – Режим доступа: <https://qna.habr.com/q/399961> (дата обращения: 11.10.20)

[3]. *Игра*, сервер и клиент / [Электронный ресурс]. – Режим доступа: <https://www.cyberforum.ru/cpp-networks/thread2148613.html> (дата обращения: 04.10.20)

[4]. *Основные* преимущества и недостатки asyncio над Tornado и Twisted / [Электронный ресурс]. – Режим доступа: <https://qna.habr.com/q/332300> (дата обращения: 13.10.20)

[5]. Thread v sEvent Loop-Сетевое программирование (язык агностик) / [Электронный ресурс]. – Режим доступа: <https://coderoad.ru/23568682/Thread-vs-Event-Loop-Сетевое-программирование-язык-агностик> (дата обращения: 24.10.20)

[6]. *Twisted* / [Электронный ресурс]. – Режим доступа: <https://8d9.ru/program/twisted> (дата обращения: 30.10.20)

Силкин Максим Игоревич – студент. E-mail: maks.klebo@gmail.com
Гуркина Е.Д. –

ОБУЧЕНИЕ НЕЙРОННОЙ СЕТИ ДЛЯ ПОИСКОВОГО ЧАТ-БОТА

Недавний успех машинного обучения во многом обязан взрывам данных в некоторых областях, таких как распознавание изображений и речи. Эти данные предоставили огромное количество примеров, которые системы машинного обучения могут использовать для повышения их производительности. В свою очередь, машинное обучение может помочь в решении социальных и экономических проблем, путем извлечения ценной информации с помощью расширенной аналитики данных. Поддержка разработки этой функции для машинного обучения требует адаптивной среды данных, основанной на открытых стандартах для обеспечения доступности данных в разных секторах.

Задачей нашего проекта является создание сервиса для автоматизации моделирования информации в социальных сетях. В сервисе будет использоваться так называемый поисковый чат-бот. В поисковых ботах используются эвристические методы для выбора ответа из библиотеки predetermined реплик. Такие чат-боты используют текст сообщения и контекст диалога для выбора ответа из predetermined списка. Контекст включает в себя текущее положение в древе диалога, все предыдущие сообщения и сохраненные ранее переменные (например, имя пользователя). Эвристика для выбора ответа может быть спроектирована по-разному: от условной логики «или-или» до машинных классификаторов. Для того чтобы обучить нашего чат-бота необходимо разобраться в глубоком обучении.

Глубокое обучение - это форма машинного обучения, в котором используется модель вычислений, которая основывается на строении мозга. Следовательно, мы называем эту модель нейронной сетью. Основной базовой единицей нейронной сети является нейрон, который на самом деле концептуально прост (рис. 1).

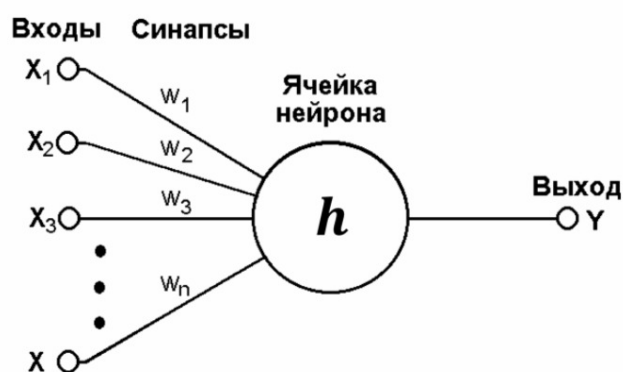


Рис. 1. Схема нейрона в нейронной сети

Каждый нейрон имеет набор входов, каждому из которых присваивается определенный вес. Нейрон вычисляет некоторую функцию на этих взвешенных входах. Линейный нейрон принимает линейную комбинацию взвешенных входов (рис. 2).

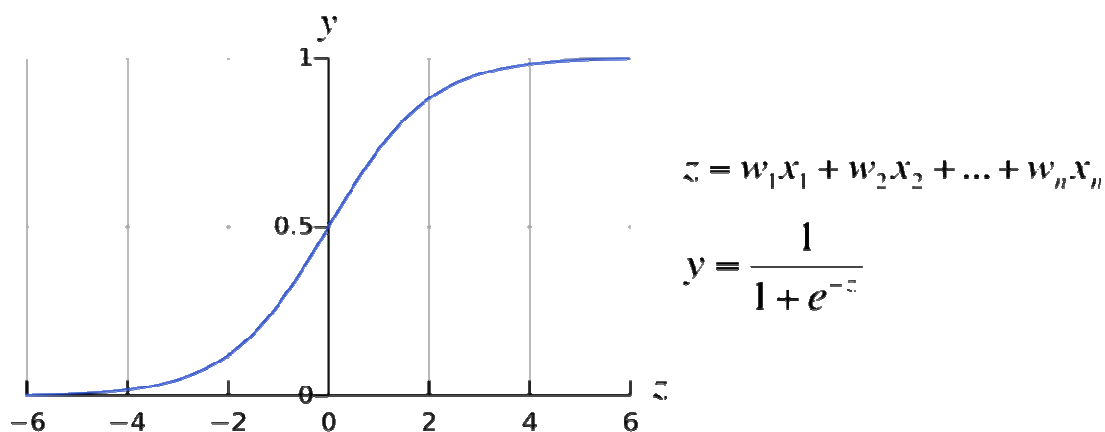


Рис. 2. Функция сигмоидального нейрона

Он подает сумму взвешенных входов в логистическую функцию. Логистическая функция возвращает значение от 0 до 1. Когда взвешенная сумма отрицательная, возвращаемое значение очень близко к 0. Когда взвешенная сумма велика и положительна, возвращаемое значение очень близко к 1. Но независимо от того, какую функцию использует нейрон, вычисляемое ею значение, передается другим нейронам в качестве входа. На практике сигмоидальные нейроны используются гораздо чаще, чем линейные нейроны, потому что они позволяют использовать более универсальные алгоритмы обучения по сравнению с линейными нейронами [1].

Нейронная сеть возникает, когда мы начинаем подключать нейроны друг к другу, к входным данным и к «выходам», которые соответствуют ответу сети на проблему обучения.

Далее следует простой пример нейронной сети (рис. 3). Пусть $w(k)_{i,j}$ – вес линии связи, соединяющей i -й нейрон в k -м слое с j -м нейроном в $k+1$ слое [3].

Подобно тому, как нейроны обычно организованы в слоях в человеческом мозге, нейроны в нейронных сетях часто организуются также в слоях, где нейроны на нижнем слое получают сигналы от входов, а нейроны в верхних слоях имеют свои выходы, соединенные с «ответом», и где обычно нет связей между нейронами в одном слое (хотя это необязательное ограничение, более сложные соединения требуют более активного математического анализа). Также отметим, что в этом примере нет соединений, которые ведут от нейрона в более высоком слое к нейрону в нижнем слое (т.е. без ориентированных циклов). Эти нейронные сети называются прямыми нейронными сетями в отличие от тех, которые называются рекурсивными нейронными сетями. Также следует учитывать:

1. Не обязательно, чтобы каждый слой имел одинаковое количество нейронов.
2. Не требуется, чтобы нейрон имел выход, подключенный к входам каждого нейрона в следующем слое.
3. Входы и выходы представляют собой векторизованные представления.
4. Слои нейронов, которые лежат между первым слоем нейронов (входной слой) и последним слоем нейронов (выходной слой), называются

скрытые слои. Это потому, что именно здесь происходит большая часть действий, когда нейронная сеть пытается решить задачу. Взглянув на действия скрытых слоев, можно многое сказать о тех функциях, которые сеть научилась извлекать из данных [2].

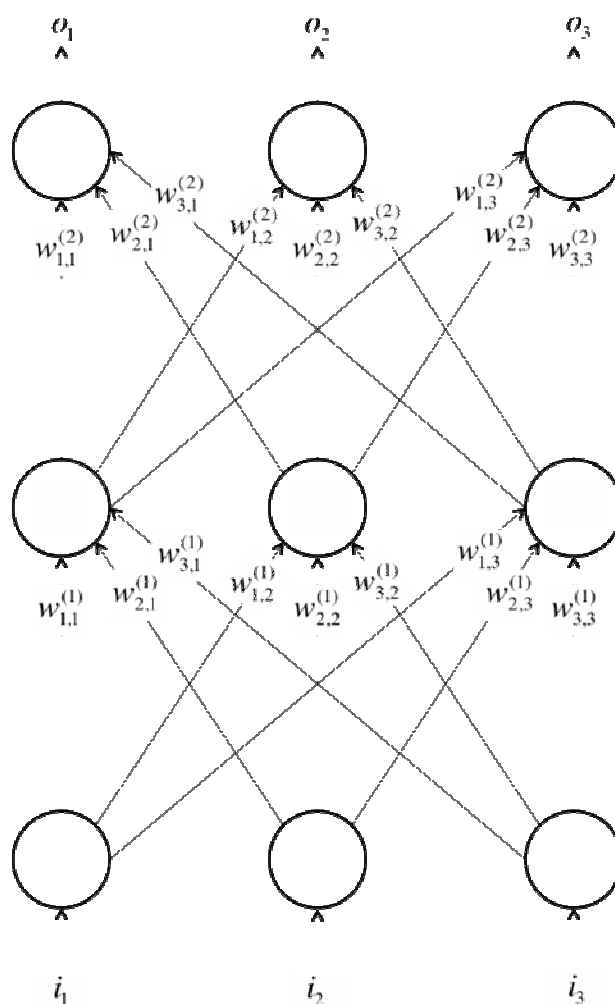


Рис. 3. Пример нейронной сети с 3 слоями и 3 нейронами на каждом слое

Список литературы

[1]. Барский А.Б. Введение в нейронные сети : учебное пособие / А.Б. Барский. – 2-е изд. – М.: ИНТУИТ, 2016. – 358 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/100684>

[2]. Краснянский М.Н., Обухов А.Д., Соломатина Е.М., Воякина А.А. Сравнительный анализ методов машинного обучения для решения задачи классификации документов научно-образовательного учреждения // Вестник вгу, серия: системный анализ и информационные технологии. – 2018. – № 3. – URL: <http://www.vestnik.vsu.ru/pdf/analiz/2018/03/2018-03-19.pdf>

[3]. Ростовцев В. С. Искусственные нейронные сети : учебник / В. С. Ростовцев. – СПб.: Лань, 2019. – 216 с. – ISBN 978-5-8114-3768-9. – Текст : элек-

тронный // Лань : электронно-библиотечная система. – URL:
<https://e.lanbook.com/book/122180>

Сергеев Вадим Владимирович — студент КФ МГТУ им. Н.Э.Баумана,
Калуга, 248000, Россия. E-mail: sergeevvadimlol@yandex.ru

Дунаев Александр Владимирович — студент КФ МГТУ им.
Н.Э.Баумана, Калуга, 248000, Россия. E-mail: sanchezzz41@mail.ru

ОСНОВНЫЕ ЭТАПЫ ПЕРЕХОДА ИЗ СИСТЕМЫ КАДРОВОГО И БУХГАЛТЕРСКОГО УЧЕТА «А1-ПЕРСОНАЛ» В СИСТЕМУ «1С»

В настоящее время система электронного кадрового и бухгалтерского учета на предприятии и управление данной системой – это одна из значительных отраслей в управленческой деятельности предприятия.

Цель данной работы – изучение и решение вопросов автоматизации процесса кадрового и бухгалтерского учета на предприятии с переходом на новую платформу.

На одном из предприятий Калужской области была поставлена задача перехода из устаревшей системы кадрового и бухгалтерского учета «А1-Персонал» в систему «1С» с целью оптимизации бухгалтерского и учетного процесса.

Программный комплекс «А1-Персонал» реализует полную автоматизацию процессов планирования, учета, движения и расчетов с персоналом. Осуществляя автоматизацию работы всех служб, относящихся к сфере работы с физическими лицами на предприятии, «А1-Персонал» логически состоит из систем, представленных на рис. 1.

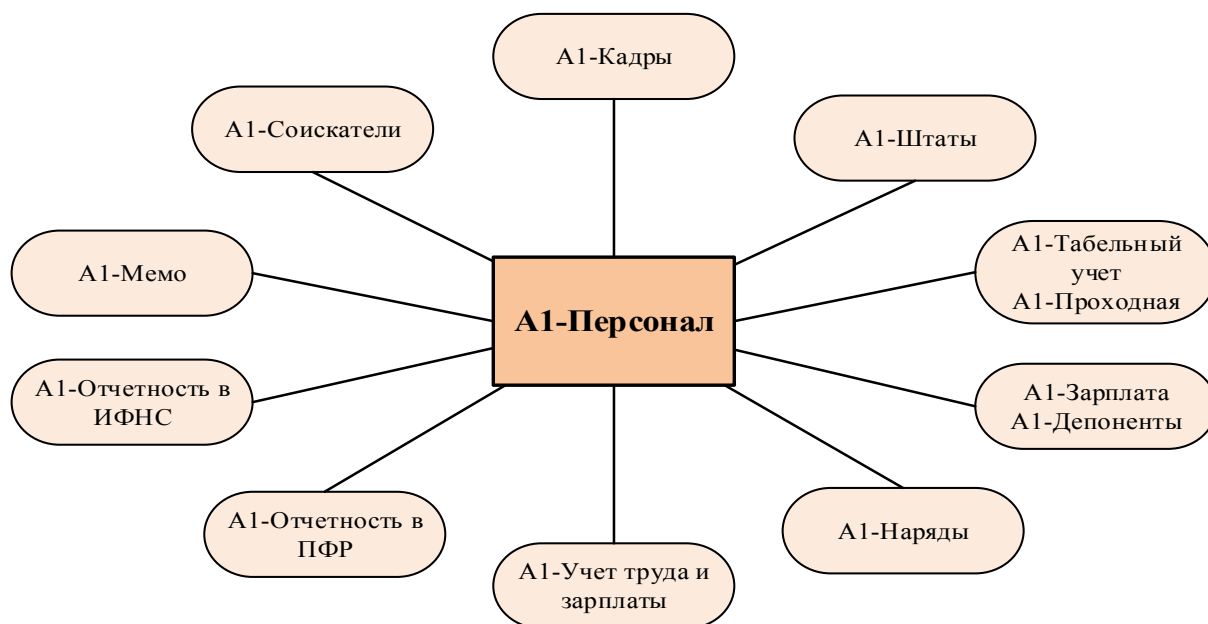


Рис. 1. Системы комплекса «А1-Персонал»

Эти системы объединены между собой и при этом могут рассматриваться как отдельные, имеющие собственные настройки и способные функционировать в любой комплектации.

Задачу перехода из системы «А1-Персонал» в систему «1С» необходимо решить с целью устранения ряда недостатков, вызванных с использованием системы «А1-Персонал».

Недостатки работы в системе А1-Персонал:

1. Использование языка программирования Natural. Natural – один из первых языков программирования четвертого поколения, который появился на рынке более четверти века назад. Именно поэтому в настоящее время язык программирования Natural является устаревшим и мало используемым, а, следовательно, имеется малое количество программистов, владеющих данным языком. Также отсутствует документация о языке Natural в свободном доступе;

2. Отсутствие работников на предприятии, которые могли бы разрабатывать обновления данной системы и исправлять технические ошибки: обновление системы приходят со сторонней организации, которая является разработчиком данного продукта;

3. Неоптимизированный процесс выгрузки бухгалтерских данных;

4. Возможность использования данного программного комплекса только на Windows XP;

5. Неудобный интерфейс комплекса «А1-Персонал» для пользователя, отсутствие эргономичного дизайна.

Для решения данной задачи были выделены основные этапы, выполнив которые можно достигнуть максимально эффективный результат перехода на новую систему:

1. Изучить систему документооборота «1С»;

2. Ознакомиться со средой «1С»;

3. Освоить ряд необходимых направлений, используемых при разработке новой системы;

4. Поэтапно внедрить реализованную систему;

5. Разработать конвертер данных из системы «А1-Персонал» в систему «1С»;

6. Загрузить данные из старой системы бухгалтерского и кадрового учета в новую систему.

Платформа «1С: Предприятие 8.3» обеспечивает эффективную работу и надежное хранение информации при одновременной работе в единой базе необходимого количества пользователей. Благодаря трёхуровневой архитектуре системы сохраняется высокая производительность при большом росте нагрузки на систему и объёмов обрабатываемых данных [1].

На базе платформы «1С: Предприятие 8.3» возможно подключить программный продукт «1С: Зарплата и управление персоналом 8», используемый для комплексной автоматизации кадрового учета и расчета заработной платы [2].

Создание системы на базе «1С» является разумным решением в качестве новой системы кадрового и бухгалтерского учета, так как данный переход имеет следующий ряд преимуществ:

1. Наличие программистов в области «1С» на данном предприятии;

2. Открытые источники получения информации по программированию на языке 1С;

3. Возможность набора новых сотрудников со знанием данного языка и платформы;
4. Возможность переделать систему под требования данного предприятия даже при покупке системы у сторонних лиц;
5. Возможность интеграции системы с рядом систем, уже внедренных на предприятии, которые базируются на платформе «1С»;
6. Возможность использования новой системы на компьютерах с современным ПО [3].

Также достаточно сложной задачей является разработка конвертера данных из системы «А1-Персонал» в систему «1С». Это связано с тем, что необходимо выгружать большое количество данных о сотрудниках, учете, все имеющиеся справочники кодов, хранящихся на огромных серверах. Данный конвертер должен быть реализован с помощью языка Natural с использованием большого количества запросов с обращением к многочисленному числу полей для извлечения данных из системы «А1-Персонал», чтобы избежать прямого взаимодействия с сервером.

Для разработки конвертера необходимо выполнить следующие задачи:

1. Изучить язык Natural;
2. Изучить структуру запросов для выгрузки данных на языке Natural;
3. Изучить имеющиеся базы данных, их поля, форматы полей и возможность обращения к ним;
4. Написать программу на языке Natural по выбору информации из каждой необходимой базы данных из системы «А1-Персонал»;
5. Написать программу переноса извлеченных данных в систему «1С» без потери и искажения информации.

Таким образом, выше была описана система «А1-Персонал», выявлены её недостатки, описаны основные этапы перехода на новую систему «1С», рассмотрены задачи разработки специализированного конвертера кадровых и бухгалтерских данных из системы «А1-Персонал» в систему «1С». В настоящее время ведется разработка новой системы бухгалтерского и кадрового учета на базе «1С: Предприятие 8.3» и «1С: Зарплата и управление персоналом 8».

Список литературы

- [1]. *Радченко М.Г.* 1С: Предприятие 8.3 практическое пособие разработчика. – М.: Издательство 1СПублишинг, 2016. – 928с. + CD.
- [2]. *Бартеньев О.В.* 1С: Предприятие: программирование для всех. – М.: Диалог-МИФИ, 2005. – 464с.
- [3]. *Лушников В.В., Бондарев А.В.* 1С: Документооборот: 200 вопросов и ответов. – М.: 1СПублишинг, 2014. – 298с.

Бояровская Алена Валентиновна – студент, бакалавр КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: egorova230598@yandex.ru

Н.А. Борсук –

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ DNSOVERHTTPS В ЦЕЛЯХ ЗАЩИТЫ ОТ ИНФОРМАЦИОННЫХ АТАК.

ОПИСАНИЕ ПРОБЛЕМЫ

Система доменных имен DNS – одна из технологий, лежащих в самой основе современного интернета. С её помощью соотносятся числовые IP-адреса и более удобные для человека доменные имена. Она построена по принципу иерархического взаимодействия DNS-серверов.

Проблема безопасности DNS заключается в том, что базовая система DNS принимает и передает любые запросы, поступающие в нее. Как во многих других решениях, которые появились на заре развития интернет-технологий, защиты от злонамеренного использования здесь нет. В те времена считалось, что главное – это простота и масштабируемость, так как интернетбыл сетью, которая связывала американские научные и военные учреждения, и подключать к ней случайных пользователей не предполагалось [4].

В результате вышеуказанной проблемы появились разные методы атак на DNS-серверы. В пример можно привести такие типы атак, как отравление кэша DNS и перехват DNS.

Отравление кэша DNS – повреждение целостности данных в системе DNS путём заполнения кэша DNS-сервера данными, не исходящими от авторитетного DNS-источника. Когда DNS-сервер получает неаутентичные данные и кэширует их для оптимизации быстродействия, он становится отравленным и начинает предоставлять неаутентичные данные своим клиентам [2].

Перехват DNS – подрыв разрешения DNS-запросов. Данная атака может быть проведена с помощью вредоносных программ, которые перекрывают TCP/IP-конфигурации компьютера, чтобы запросы отправлялись на DNS-сервер злоумышленника, либо через изменение поведения доверенного DNS-сервера так, чтобы оно не соответствовало стандартам Интернета. Эти изменения могут быть сделаны в злонамеренных целях, таких как фишинг, или в корыстных целях Интернет-провайдером, направляющими веб-трафик пользователя на собственные веб-серверы для показа рекламы, сбора статистики или других целей провайдера; и поставщиками услуг DNS для блокирования доступа к выбранным доменам как форма цензуры [2].

Для борьбы с этими и подобными атаками Инженерный совет интернета разработал набор расширений DNSSEC, который добавил к DNS-запросам подпись-аутентификацию на основе криптографии с открытым ключом.

DNSSEC (англ. Domain Name System Security Extensions) – набор расширений IETF протокола DNS, позволяющих минимизировать атаки, связанные с подменой DNS-адреса при разрешении доменных имён. Он направлен на предоставление DNS-клиентам аутентичных ответов на DNS-запросы и обеспечение их целостности. При этом используется криптография с открытым ключом [5].

Несмотря на то, что DNSSEC гарантирует аутентичность и целостность данных, данный набор расширений решает только часть проблемы – приватность остается под угрозой. В борьбе за эту цель логичным средством выступает шифрование. Вопрос заключается в том, как именно его реализовать.

Несколько групп разработчиков предложили свои варианты технологических решений. Среди них существуют те, которые используют оригинальные способы шифрования, например DNSCrypt или DNSCurve, в котором применяется шифрование с использованием эллиптических кривых. Но решения, оказавшиеся в итоге более популярными, опираются на широко распространенный протокол безопасности TLS. Наиболее популярным решением на данный момент является DoH (DNS over HTTPS).

ПРИНЦИП ДЕЙСТВИЯ DOH

При использовании данного протокола, DoH-клиент обращается к DNS-серверу, который должен обязательно поддерживать DoH через стандартный TCP-порт 443. Шифрование соединения не позволяет сетевым посредникам проследить, какие адреса ищет браузер или же подделать ответ, все запросы конфиденциальны и защищены между ПК и доверенным DNS Resolver. Далее DoH-клиент получает сертификат сервера и проверяет его, а затем генерирует симметричный ключ шифрования, используя алгоритм шифрования, который поддерживают обе стороны, для фактического шифрования данных. Трафик через браузер идет, обменяв все настройки DNS на уровне сети и провайдера, по HTTPS попадает сразу к поддерживающему DoH DNS Resolver, на котором и идет обработка запросов через Web API. Говоря простым языком, принцип работы протокола DNS over HTTPS заключается в шифровании запросов к DNS-серверу и ответов на них. Имена удаленных серверов, к которым обращается пользователь с использованием DoH, скрываются.

НЕДОСТАТКИ DOH

Первой проблемой DNS over HTTPS можно назвать снижение безопасности работы в сети Интернет. Системным администратором станет сложнее блокировать вредоносные сайты, так как их имена невозможно изъять из HTTPS-трафика, а обычные пользователи лишатся возможности родительского контроля в браузерах своих устройств.

К примеру, Законодательство Великобритании, так же, как и в России, обязывает интернет-провайдеров осуществлять блокировку запрещенных сайтов. С использованием протокола DoH фильтровать трафик становится практически невозможно. Против популяризации протокола выступают Центр правительственной связи Англии (GCHQ) и фонд Internet Watch Foundation (IWF), их задача заключается в ведении реестра заблокированных ресурсов.

Вторая проблема использования DNS over HTTPS в появлении новых вредоносных программ, которые используют особенности протокола. Так, например, в июле этого года специалисты по информационной безопасности Netlab обнаружили новый вирус Godlua, использующий DoH для проведения DDoS-атак[1]. Вредоносная программа из DoH получает текстовые записи DNS (TXT) и URL-адреса управляющих серверов. Угроза кибербезопасности

заключается в том, что популярные антивирусные решения не могут распознать зашифрованные DoH-запросы. Дальше будут появляться новые вирусы, и ситуация начнет усугубляться.

ПОДДЕРЖКА РАЗВИТИЯ DoH

На основе отчетов крупных IT-компаний, которые поддержали разработку протокола, можно сделать положительный прогноз о развитии технологии. Mozilla поддерживает данную технологию с лета 2018 года. В поддержку Mozilla высказались крупные СМИ и некоторые интернет-провайдеры. В частности, в BritishTelecom считают, что новый протокол не повлияет на фильтрацию контента и повысит безопасность британских пользователей. Также за внедрение DNS over HTTPS выступили облачные провайдеры, например Cloudflare. Они уже предлагают DNS-сервисы на базе нового протокола. Также Google имеет свою версию DoH-сервиса. В Google надеются, что он повысит безопасность персональных данных в сети и защитит от MITM-атак [3].

В заключении хочется отметить, что технология DNS over HTTPS, несмотря на её недостатки, достаточно перспективная и может стать частью массового набора интернет-технологий, на это уйдет не одно десятилетие, как это было с набором расширений DNSSEC.

Список литературы

[1]. *Alex Turing, Genshen Ye*. An Analysis of Godlua Backdoor. – URL: <https://blog.netlab.360.com/an-analysis-of-godlua-backdoor-en/> (дата обращения: 25.10.2020)

[2]. *Chris Sanders*. Understanding Man-In-The-Middle Attacks. Part2: DNS Spoofing. – URL: <http://techgenix.com/Understanding-Man-in-the-Middle-Attacks-ARP-Part2/> (дата обращения: 25.10.2020)

[3]. *Dan Goodin*. A DNS hijacking wave is targeting companies at an almost unprecedented scale. – URL: <https://arstechnica.com/information-technology/2019/01/a-dns-hijacking-wave-is-targeting-companies-at-an-almost-unprecedented-scale/> (дата обращения: 25.10.2020)

[4]. *Donald E. Eastlake 3rd*. Detached Domain Name System (DNS) Information. – URL: <https://tools.ietf.org/html/rfc2540/> (дата обращения: 25.10.2020)

[5]. *Paul Mockapetris*. Domain names—concepts and facilities. – URL: <https://tools.ietf.org/html/rfc1034> (дата обращения: 25.10.2020)

Макаров Георгий Павлович – студент, бакалавр КФ МГТУ им. Н.Э. Баумана. E-mail: uin6x6@gmail.com

Е.В. Вершинин –

ПРОЕКТИРОВАНИЕ УСТРОЙСТВА ДЛЯ ДОМАШНЕГО ТЕРМОСТАТИРОВАНИЯ

Введение. Большинство современных частных домов отапливаются за счет газовых котлов. Для поддержания комфортной температуры, а также предотвращения замораживания труб в отопительной системе, в период отъезда, используются терморегуляторы.

Методы терморегулирования. В зависимости от комплектации котла, есть два способа управления отоплением:

- 1) Включение и выключение горелки с помощью реле.
- 2) Постоянная и плавная регулировка мощности пламени горелки через протокол передачи данных между котлом и терморегулятором.

В первом случае, при срабатывании реле, котел начинает свою работу сразу на полной мощности, что приводит к резкому нагреву радиаторов. При достижении заданной температуры происходит выключение горелки, но из-за оставшегося тепла в радиаторах, воздух в комнатах продолжает нагреваться, тем самым переходя верхнюю границу комфортной температуры. Обратная ситуация возникает при прохождении нижней границы от отклонения заданной температуры. Кроме того, из-за долгого нагрева системы тепло будет идти определенное время, что способствует дальнейшему охлаждению помещения.

Рассмотрим второй метод терморегулирования, термостат выключает и включает горелку только при выходе за пределы гистерезиса. В промежутке между ними он модулирует мощность горения, приспособившись к текущей потребности в тепле. Таким образом достигается сохранение температуры на заданную величину при минимальных энергозатратах. Недостатками терморегуляторов с данным принципом работы являются отсутствие единого стандарта протокола связи, а также высокая цена.

Задачи устройства. Терморегулятор должен выполнять следующие задачи:

- 1) Поддерживать заданную температуру с точностью $\pm 0,5^{\circ}\text{C}$.
- 2) Приспосабливаться к изменяющимся условиям.
- 3) Работать согласно расписанию по часам и дням недели.
- 4) Управляться удаленно.
- 5) Демонстрировать данные с датчиков.

Реализация. На рис. 1 представлена схема соединения компонентов. Вычислительным блоком устройства является плата NodeMCU (U1) на основе микроконтроллера ESP8266 [1]. Данное решение позволяет реализовывать работу с сетью WIFI без подключения дополнительных модулей, прочитывать данные с цифровых датчиков и управлять четырнадцатью портами ввода-вывода. Символьный LCD 1602 дисплей (U2) выводит данные о текущем состоянии работы контроллера, полученную с датчиков информацию и ошибки, при их обнаружении. Подключение к плате (U1) осуществляется по шине I²C

(ПК) с помощью I²C преобразователя PCF8574 [2]. Датчик BME280 (U3) служит для измерения температуры и влажности воздуха, а также атмосферного давления. Благодаря подключению по SPI интерфейсу происходит более быстрая передача данных, в сравнении с I²C. Для управления котлом используется модуль реле. Питание производится от любого источника 5V.

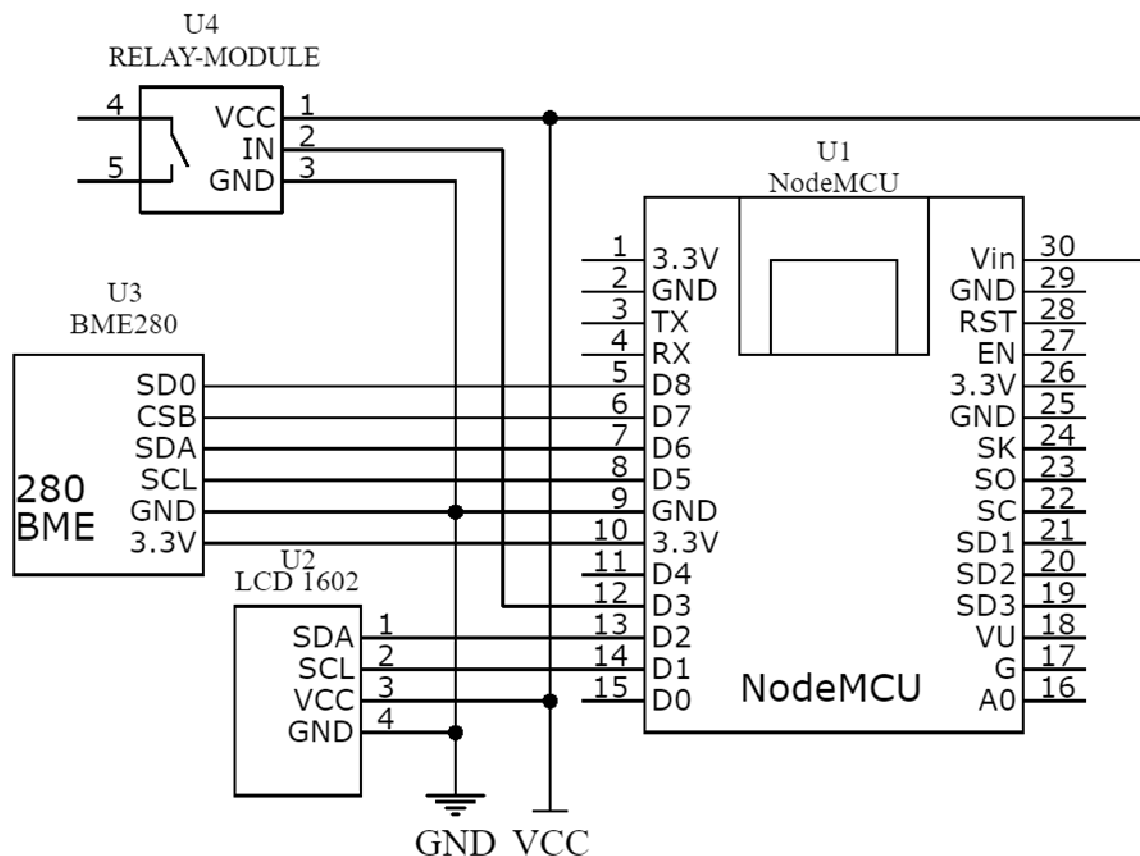


Рис. 1. Принципиальная схематерморегулятора

Алгоритм работы. После включения питания микроконтроллер опрашивает подключенные модули на предмет ошибок и неисправностей. Следующим шагом происходит попытка подключения к Wi-Fi сети. В случае если подключение не удалось устройство переходит в режим точки доступа. В этом случае создается новая Wi-Fi сеть. При подключении к ней другого устройства (смартфона, ПК) открывается HTML страница конфигурирования, где задаются параметры желаемой к подключению сети. Далее устройство входит в бесконечный цикл работы, в котором температурные значения, полученные с датчика, сравниваются с заданными «комфортными» и исходя из условий решается, включить отопление или нет. Устройство постоянно прослушивает UDP пакеты, если пакет соответствует требованиям, он распаковывается и записывается в ОЗУ. Некоторые данные, такие как: «комфортная» температура, расписание, установленные таймеры, записываются в энергонезависимую память (EEPROM), для их восстановления и загрузки, в случае отключения питания.

Возможности для улучшения. Терморегулятор имеет большой потенциал для развития в системах умного дома. Контролер имеет возможность сканировать другие устройства в локальной сети. Таким образом получая температурные значения из определенных комнат, что позволяет лучшим образом достичь предпочтительной температуры при минимальных энергозатратах. Статистика данных за определённый период времени позволит узнать эффективность отопительной системы и неисправности в контурах отопления. Благодаря информации из отдельно взятой комнаты можно оптимально отрегулировать напор в контуре, что способствует сокращению расходов.

Список литературы

[1]. *Начало работы с ESP8266 NodeMcu v3 Lua с WiFi.* – URL: <https://arduinomaster.ru/platy-arduino/esp8266-nodemcu-v3-lua/> (дата обращения 07.11.2020)

[2]. *PCF8574 datasheet.* – URL: https://www.nxp.com/docs/en/datasheet/PCF8574_PCF8574A.pdf (дата обращения 07.11.2020)

Разгоев Артем Анзорович – студент КФ МГТУ им. Н.Э. Баумана.
E-mail: razgovevartem@gmail.com

Гагарин Юрий Евгеньевич – заведующий кафедрой, канд. техн. наук
КФ МГТУ им. Н.Э. Баумана. E-mail: Yriigagarin@yandex.ru

РАЗРАБОТКА ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В МОДУЛЕ ОБНАРУЖЕНИЯ СТОРОННИХ ПРЕДМЕТОВ В СИСТЕМЕ АВТОДОСМОТРА

Модуль распознавания будет являться частью микросервесной Rest архитектуры. В общем случае REST является очень простым интерфейсом управления информацией без использования каких-то дополнительных внутренних прослоек [1]. Каждая единица информации однозначно определяется глобальным идентификатором, таким как URL.

В качестве языка программирования выбран Java-строго типизированный объектно-ориентированный язык программирования, разработанный компанией Oracle. Программы на Java транслируются в байт-код Java, выполняемый виртуальной машиной Java – программой, обрабатывающей байтовый код и передающей инструкции оборудованию как интерпретатор [2].

Достоинством подобного способа выполнения программ является полная независимость байт-кода от операционной системы и оборудования, что позволяет выполнять Java-приложения на любом устройстве, для которого существует соответствующая виртуальная машина.

Модуль распознавания должен взаимодействовать со всей системой автодосмотра каким-либо защищенным образом. Наиболее надежным и гибким методом представляется авторизация при помощи технологии JWT (JSON WebToken) [3]. Он считается одним из безопасных способов передачи информации между двумя участниками. Для его создания необходимо определить заголовок (header) с общей информацией по токену, полезные данные (payload), такие как id пользователя, его роль и т.д. и подписи (signature). Данный механизм не только позволяет ограничить доступ к модулю, но и настроить использование ролей в системе [3].

При помощи фильтра происходит аутентификация пользователей (рис. 1). Также необходимо произвести cors-конфигурацию и позволить делать запросы только авторизованным пользователям.

```
@Override
protected void configure(HttpSecurity http) throws Exception {
    http
        .cors().configurationSource(request -> corsConfiguration()) CorsConfigurer <HttpSecurity>
        .and() HttpSecurity
        .csrf().disable() HttpSecurity
        .sessionManagement().sessionCreationPolicy(SessionCreationPolicy.STATELESS) SessionManagementConfigurer <HttpSecurity>
        .and() HttpSecurity
        .authorizeRequests() ExpressionUrlAuthorizationConfigurer <H>.ExpressionInterceptUrlRegistry
        .anyRequest().authenticated() ExpressionUrlAuthorizationConfigurer <H>.ExpressionInterceptUrlRegistry
        .and() HttpSecurity
        .addFilter(new JwtCreateFilter(authenticationManager()));
}
```

Рис. 1. Фильтр аутентификации пользователей

После получением клиентом токена необходимо проверять его в заголовке при каждом запросе к сервису [3]. Для проверки наличия токена в заголовке запроса необходимо создать класс, отвечающий за успешную авторизацию.

Данный класс будет принимать в себя весь запрос и получать нужный заголовок. После успешного сопоставления значений пользователь будет допущен и ему откроется весь функционал модуля обнаружения сторонних предметов (рис. 2).

```
private UsernamePasswordAuthenticationToken getAuthentication(HttpServletRequest request) {  
  
    String token = request.getHeader("Authorization");  
    if (token != null) {  
  
        System.out.println("token is not null");  
  
        try {  
            String username = JWT.require(Algorithm.HMAC512("secret")).build().verify(token.replace("Bearer ", "")).getSubject();  
            System.out.println(username);  
  
            return new UsernamePasswordAuthenticationToken(  
                username, credentials: null, new ArrayList<>());  
        } catch (Exception e) {  
            // In case of failure. Make sure it's clear; so guarantee user won't be authenticated  
            System.out.println("wrong token");  
            SecurityContextHolder.clearContext();  
            return null;  
        }  
    }  
    else {  
        System.out.println("token is null");  
        return null;  
    }  
}
```

Рис. 2. Процесс проверки токена

В ходе статьи, был разработан механизм защищенного информационного взаимодействия в системе автодосмотра. Также рассмотрены преимущества использования JWTтокена в качестве основной технологии защиты и разграничения прав доступа.

Список литературы

[1]. Крысин И.А., Погорелов Н.К., Чухраев И.В. Реализация системы контроля и управления доступом в высшем учебном заведении.// Электромагнитные волны и электронные системы. – 2019. – Т. 24. – № 7. – С. 43-47.

[2]. Монахов В. Язык программирования Java и среда NetBeans (+ CD-ROM) / В. Монахов. – М.: БХВ-Петербург, 2012. – 720 с.

[3]. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. – М.: ГЛТ, 2016.– 280 с.

Петрушин Александр Андреевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: petrushin.mail@yandex.ru

Чухраев Игорь Владимирович – преподаватель КФ МГТУ им. Н.Э. Баумана. E-mail: chukhraev@bmstu-kaluga.ru

РАЗРАБОТКА МОДУЛЯ АВТОРИЗАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ДЛЯ СТУПЕНЕЙ НАЧАЛЬНОЙ ШКОЛЫ

Современный мир с каждым днём становится все более зависимым от компьютерных технологий, так как они используются во всех сферах общественной жизни. Поэтому использование нововведений, позволяющих совершенствоваться в данной области на уроках в начальной школе, является не только требованием сегодняшнего дня, но и объективным, естественным этапом развития.

Разработка информационной системы представляет собой совокупность модулей (микросервисов), взаимодействующих друг с другом посредством REST архитектуры, а именно: модуль авторизации, модуль личного кабинета, модуль электронного дневника, модуль электронного журнала, модуль расписания и модуль напоминаний. В данной статье представлены основные этапы разработки модуля авторизации в информационной системе для ступеней начальной школы.

Для реализации окна авторизации будем использовать технологию WPF (Windows Presentation Foundation), которая является частью экосистемы платформы .NET и представляет собой подсистему для построения графических интерфейсов [1].

Основными преимуществами, исходя из которых была выбрана данная технология, являются:

- Использование традиционных языков .NET-платформы – C# и VB.NET для создания логики приложения

- Возможность декларативного определения графического интерфейса с помощью специального языка разметки XAML, основанном на xml и представляющем альтернативу программному созданию графики и элементов управления, а также возможность комбинировать XAML и C#/VB.NET

- Независимость от разрешения экрана: поскольку в WPF все элементы измеряются в независимых от устройства единицах, приложения на WPF легко масштабируются под разные экраны с разным разрешением

- Создание приложений под множество ОС семейства Windows - от Windows XP до Windows 10 [2].

Для того чтобы разработать окно авторизации пользователя в приложении WPF необходимо создать страницу, которая имеет следующие компоненты:

- четыре компонента «Label» (текст). Данные поля нужны для отображения надписей на рабочей форме, в данном случае «Введите Ваше имя и пароль», «Логин», «Пароль», «Забыли пароль?» [3].

- компонент «TextBox» (поле ввода текста) с наименованием «textBox_login». Позволяет вносить текст в специальное поле ввода, необходим для указания логина пользователя

- компонент «PasswordBox» (поле ввода текста скрывающие введенный текст) с наименованием «password». Данное поле, позволяет вносить текст в специальное поле для ввода, скрывая введенный текст специальным символом

- компонент «Button» (кнопки) с прикрепленными функциями. Компонент типа «Button» предназначен для создания кнопок на форме, которые в свою очередь способны обрабатывать большое количество событий

Таким образом, изменив стили данных компонентов, делается визуальная часть окна авторизации, представленная на рис. 1.

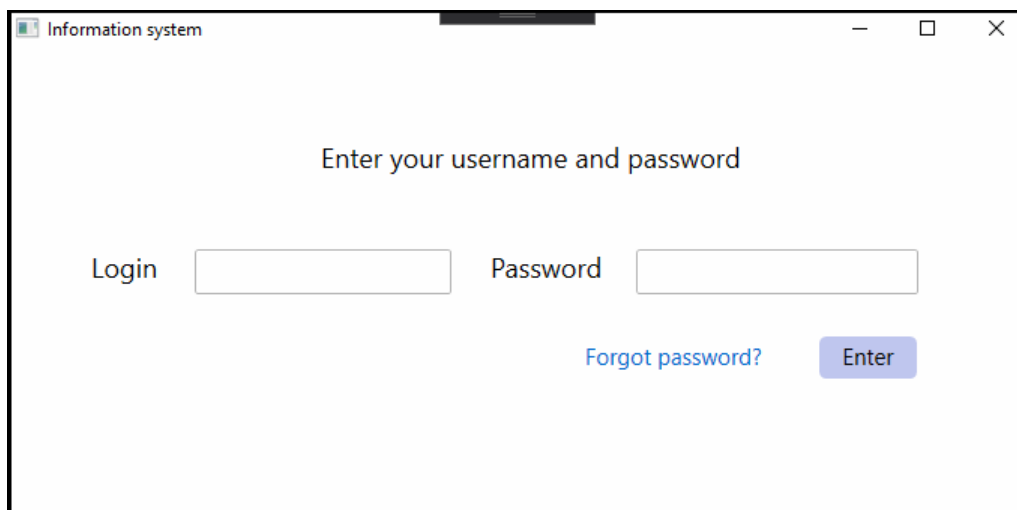


Рис. 1. Окно авторизации пользователя

Также при создании страницы будет автоматически сгенерирован код обработчиков кнопки и ссылки для восстановления пароля, показанные на рис. 2.

```
public partial class MainWindow : Window
{
    1 reference
    public MainWindow()
    {
        InitializeComponent();
    }

    1 reference
    private void Enter_Click(object sender, RoutedEventArgs e)
    {
    }

    1 reference
    private void hyperlink_Click(object sender, RoutedEventArgs e)
    {
    }
}
```

Рис. 2. Код обработчиков кнопки и ссылки

Теперь необходимо написать алгоритм проверки введенных пользователем данных, содержащий проверку заполняемости всех полей, существования записи в БД. Если запись существует, пользователь авторизуется и будет выведено всплывающее окно. Данный алгоритм представлен на рис. 3, при нажа-

тии на кнопку «Enter» и, также требуется заполнить обработчик ссылки и написать метод выборки данных из базы данных. [4]

```
1 reference
private void Enter_Click(object sender, RoutedEventArgs e)
{
    LoadingImages loadingImages = new LoadingImages();
    MainWindow mainWindow = new MainWindow();

    if (login.Text.Length > 0 )
    {
        if (password.Password.Length > 0)
        {
            DataTable dt_user = Select("SELECT * FROM [dbo].[Users] WHERE [login] = '" + login.Text +
                                     "' AND [password] = '" + password.Password + "' ");
            if (dt_user.Rows.Count > 0)
            {
                System.Windows.MessageBox.Show("User is logged in");
            }
            else System.Windows.MessageBox.Show("User not found");
        }
        else System.Windows.MessageBox.Show("Enter the password");
    }
    else System.Windows.MessageBox.Show("Enter the login");
}

1 reference
private void hyperlink_Click(object sender, RoutedEventArgs e)
{
    Process.Start("http://corepartners.ru/");
}
```

Рис. 3. Алгоритм проверки данных, обработчик ссылки и метод выборки из БД

В результате при запуске приложения открывается окно, показанное на рис. 4, при введении в котором правильного логина и пароля, выпадает уведомление о том, что пользователь авторизован (Userisloggedin). Соответственно при введении неверных данных, на экране появится сообщение – пользователь не найден (Usernotfound). [5]

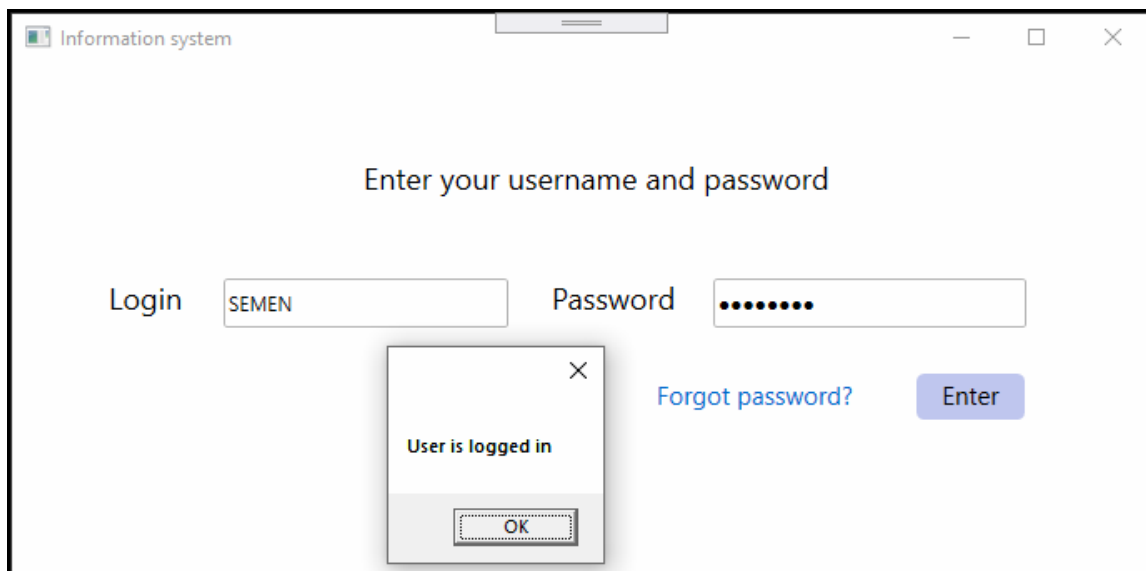


Рис. 4. Окно подтверждения авторизации пользователя

Таким образом, выше были рассмотрены основные преимущества технологии WindowsPresentationFoundation для реализации модуля авторизации в рамках разработки информационной системы для ступеней начальной школы. Представлен один из вариантов реализации окна авторизации пользователя.

Список литературы

[1]. *Назаров С.В.* Современные операционные системы : учебное пособие / С.В. Назаров, А.И. Широков. – 3-е изд. – М., Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 351 с.

[2]. *Мак-Дональд М.* WPF: WindowsPresentationFoundation в .NET 4.0 с примерами на С# 2010 для профессионалов, 2018

[3]. *Технологии* создания электронных обучающих средств [Электронный ресурс].

[4]. *Рихтер* «CLR via С#. Программирование на платформе Microsoft .NET Framework 4.0 на языке С#»

[5]. *Раскин Дж.* Интерфейс: новые направления в проектировании компьютерных систем. – Символ-плюс, 2017

Кургузов Семен Дмитриевич – студент, бакалавр; ООО Коре Партнерс Софт. E-mail: ksd40@yandex.ru

Гартман Вадим Алексеевич – студент, бакалавр. E-mail: vadim.gartman@yandex.ru

Борсук Наталья Александровна – доцент кафедры «Информационные системы и сети», канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: borsuk.65@yandex.ru

АВТОМАТИЗАЦИЯ В МАШИННОМ ОБУЧЕНИИ

Автоматизация – это технология, благодаря которой какой-либо процесс или какая-либо процедура выполняются с минимальным участием человека. Благодаря автоматизации можно добиться как повышения производительности труда, так и снижения себестоимости готовой единицы продукта. С течением времени методы автоматизации только совершенствуются, что позволяет их применять в новых областях. Например, в течение последних десятиков лет они развились от простых механизмов до роботов, которые активно используются в промышленности. В наши дни автоматизация уже затрагивает не только физический труд, но и интеллектуальный. Ярким примером является машинное обучение, которое является подразделом искусственного интеллекта, изучающего способы и методы создания алгоритмов. Ведущие компании, такие как Google и Yandex активно применяют его в множестве своих продуктов.

Языком для разработки был выбран Python ввиду того, что он обладает большим количеством готовых решений. Для работы с машинным обучением использовались библиотеки scikit-learn и Hyperopt. Scikit-learn – это надежная и удобная библиотека, которая является реализацией целого ряда алгоритмов для обучения с учителем (Supervised Learning) и обучения без учителя (Unsupervised Learning) через интерфейс для языка программирования Python. Для работы с гиперпараметрами использована библиотека Hyperopt.

Решение задач в области обработки данных и машинного обучения имеет большой список факторов, который тем или иным образом влияет на процесс.

К списку можно отнести:

- Модели, полученные в результате работы алгоритмов машинного обучения, имеют большую погрешность и являются неточными;
- Механизмы обработки и анализа требуют постоянной модернизации и улучшения ввиду постоянно поступающей новой информации;
- При обработке и анализе данных приходится принимать огромное количество больших и малых решений. К примеру, от определения необходимости нормализовать данные до того, каким методом это лучше сделать.
- Ввиду недостатка априорных знаний о данных и зависимостях, всегда присутствует элемент исследования.

Наличие вышеописанных факторов усложняет как решение задач машинного обучения, так и их автоматизацию, но в то же время, вычислительные возможности с течением времени только растут и становятся более доступными. И это позволяет подключить к процессу решения задачи большее количество ресурсов.

Принимая во внимание вышесказанное, становится ясно, что процесс получения пайплайна обработки и анализа данных – это сложная систе-

ма.Pipeline (пайплайн) – это процесс разработки (подготовки, производства), программный конвейер. Данный термин мы будем далее использовать [1].

Сложная система – набор разнообразных процессов и вещей, её отличительной чертой, является наличие большого количества взаимодействующих элементов, а также нелинейных связей между ними. Зачастую это приводит к сложно воспроизводимым процессам, например к самоорганизации.

Согласно стандарту CRISP-DM, жизненный цикл проекта, имеющего анализ данных, включает в себя:

- осознание бизнес-задачи;
- изучение и понимание данных;
- обработка данных;
- моделирование;
- оценка качества;
- практическое применение.

Существующие библиотеки делают упор на автоматизацию моделирования, но стоит отметить, что изменение подхода к автоматизации обработки данных позволит охватить большее количество этапов.

Большая часть способов решения задач машинного обучения основано на минимизации функции потерь.[2] J (1), а также на максимизации функции правдоподобия L (2), с целью получения оценки параметров θ_m , который основан на имеющейся выборке, т.е. обучающего набора данных y_t .

$$\bar{\theta}_m = \operatorname{argmin}_{\theta_m} (J(y_t; \theta_m)) \quad (1)$$

$$\bar{\theta}_m = \operatorname{argmax}_{\theta_m} (L(y_t; \theta_m)) \quad (2)$$

Приступим к автоматизации процесса выбора способа обработки данных, выбора модели и выбору гиперпараметров к ней с условием что они должны быть близки к оптимальным. Оптимизация гиперпараметров – задача машинного обучения по выбору набора оптимальных гиперпараметров для обучающего алгоритма. Гиперпараметр – переменная, содержащая предположения, веса или скорости обучения для разных видов данных, требующихся в схожих видах машинного обучения [3]. Их следует настраивать так, чтобы модель могла оптимально решить задачу обучения.

Перенесем описанное на пример, в котором происходит выбор между двумя методами обработки данных `standardscaler` и `quantilescaler`, а также двумя моделями `randomforest` и `neuralnetwork`. В примере (рис.1) структура представлена как дерево:

Каждый выбор является параметром системы. Дерево является пространством возможных параметров. Данный способ представления проблемы позволяет сформулировать задачу получения итогового пайплайна, включающего методы обработки данных, модели и их параметры, как процесс минимизации (4), или максимизации функции (3).

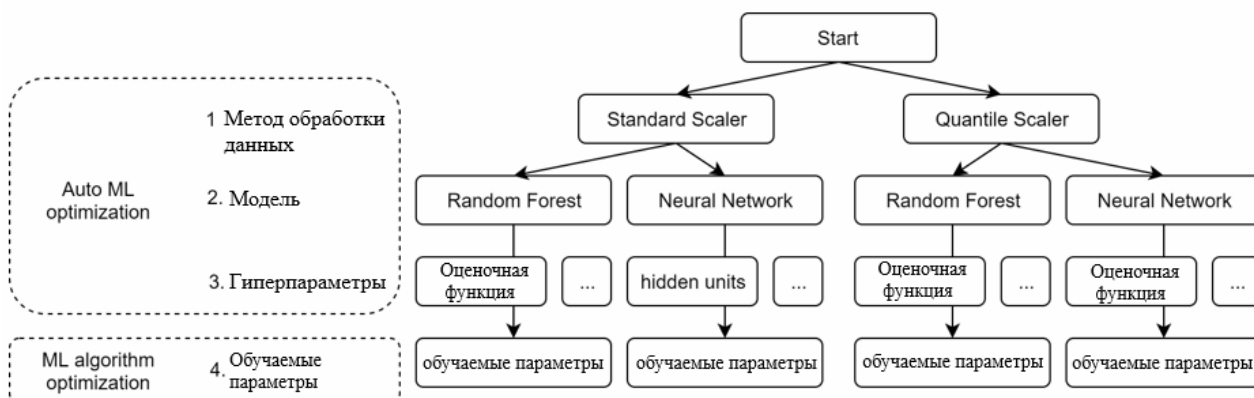


Рис. 1. Дерево выбора между двумя методами обработки данных «randomforest» и «neuralnetwork»

$$\hat{\omega} = \operatorname{argmax}_{\omega} (L(y_t, y_{cv}; \omega)) \quad (3)$$

$$\hat{\omega} = \operatorname{argmin}_{\omega} (J(y_t, y_{cv}; \omega)) \quad (4)$$

Плюсами данного способа автоматизации процесса обучения являются:

- упрощение процесса машинного обучения за счет его автоматизации, что дает возможность применять некоторые способы большому числу работников, в том числе и не являющимися специалистами в области машинного обучения;

- подбор большего числа параметров системы при наличии одной входной точки в рамках одного процесса автоматизации;

- автоматизация рутинных задач.

К минусам можно отнести:

- увеличение числа параметров, что ведет к росту их пространства.

В результате, это приводит к развитию алгоритмов и увеличению количества необходимых вычислительных ресурсов необходимых для их работы;

- полученное решение не всегда является гибким, что негативно влияет на полученный результат, а также на дальнейшие его улучшения и модификации;

- процесс оптимизации зачастую затруднен, т.к. пространство параметров ω нелинейно и обладает сложной структурой.

Чтобы уйти от ряда недостатков и сохранить как можно больше преимуществ, можно использовать подход semi-automl. Данный способ является представителем полуавтоматических алгоритмов [4]. Существование полуавтоматической системы, имеющей возможность конфигурирования, позволяет создавать типовые сценарии, наиболее подходящие для решения определенных задач. С этой целью, был настроен и использован инструмент, решающий задачу полуавтоматического машинного обучения на основе гибридной функционально-декларативной системы конфигурации. Выбранный способ конфигурации использует как стандартные типы данных, так и функции из библиотек машинного обучения. Использование инструмента позволяет автоматизировать выбор моделей и их гиперпараметров, процесс создания простых мето-

дов обработки данных, базовое конструирование признаков. Далее продемонстрирована формализация примера, рассмотренного ранее (рис. 2). В примере использованы модели из `sk-learn` и `hyperopt` для оптимизации и распределения параметров.

```
'preprocessing': {
    'scaler': hp.choice('scaler', [
        {
            'func': RobustScaler,
            'params': {
                'quantile_range': (10, 90)
            }
        },
        {
            'func': StandardScaler,
            'params': {
                'with_mean': True
            }
        }
    ]),
},

'model': hp.choice('model', [
    {
        'func': RandomForestClassifier,
        'params': {
            'max_depth': hp.choice('r_max_depth', [2, 5, 10]),
            'n_estimators': hp.choice('r_n_estimators', [5, 10, 50])
        }
    },
    {
        'func': MLPClassifier,
        'params': {
            'hidden_layer_sizes': hp.choice('hidden_layer_sizes', [1, 10, 100]),
            'learning_rate_init': hp.choice('learning_rate_init', [0.1, 0.01])
        }
    }
]),
])
```

Рис. 2. Формализация примера

После применения полученных знаний на практике было выявлено, что не часто можно встретить полное отсутствие автоматизации, так как даже самый простой перебор значений одного гиперпараметра в цикле – это уже шаг к автоматизации, но полная автоматизация всего процесса построения пайплайна на сегодняшний день не достижима. Стоит отметить, что в процессе разработки множества передовых проектов просто необходимо применение разных подходов к процессу автоматизации. Одним из самых удобных и универсальных для применения способов является полуавтоматический. Использование данного метода машинного обучения позволяет наиболее эффективно использовать ресурсы, выделенные разработчику.

Список литературы

[1]. *Oliver Theobald*. Machine Learning For Absolute Beginners: A Plain English Introduction 2018. – [Электронный ресурс] Режим доступа: <https://arxiv.org/pdf/1503.04069.pdf>.

[2]. *Петер Флах*. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных / Петер Флах. – СПб.: Питер, 2018. – С. 285–296.

[3]. *Андреас Мюллер, Сара Гвидол*. Введение в машинное обучение с помощью Python // Компьютерная лингвистика и обработка естественного языка. – [Электронный ресурс]. Режим доступа: <http://www.vestnik.vsu.ru/pdf/analiz/2015/04/2015-04-21.pdf>.

[4]. *Бурков А.В.* Машинное обучение без лишних слов / А.В. Бурков. – СПб.: Питер, 2019. – 273 с.

Коротков Глеб Александрович – студент КФ МГТУ им. Н.Э.Баумана, Калуга, 248000, Россия. E-mail: gleb-ukhta@yandex.ru

Научный руководитель: Вершинин Евгений Владимирович. КФ МГТУ им. Н.Э. Баумана. E-mail: 248000, Россия. E-mail: yevgeniyv@mail.ru

ИССЛЕДОВАНИЕ ПЛАТФОРМ ДЛЯ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Системы дистанционного обучения достаточно давно известны широкому кругу людей. С помощью дистанционных образовательных технологий можно не только переложить на плечи компьютера ряд рутинных педагогических действий, но и организовать по-настоящему качественное, индивидуальное, дифференцированное обучение [1]. В рамках текущей эпидемиологической ситуации эта задача тем более актуальна.

В рамках данной статьи будут рассмотрены критерии, которые в значительной степени упростят выбор платформы для осуществления дистанционного обучения [2], а также приведены примеры данных платформ.

Первым важным критерием нужно указать наличие или отсутствие системы создания контента. Это может быть важно, так как некоторые платформы, такие как, например, Memberlux, который позволяет продавать учебный контент: лекции, видеокорсы, подкасты, но не создавать его.

Другим важным критерием может как раз стать встроенная система продажи курсов. Для коммерческой деятельности это сильно упростит процесс передачи учебного контента от продавца покупателю.

Следующим критерием станет наличие геймификации. Геймификация – это использование игровых подходов, которые широко распространены в компьютерных играх, для неигровых процессов, что позволяет повысить вовлечённость участников в решение прикладных задач [3]. Это свойство просто необходимо платформам для обучения детей, так как многократно усиливает эффект обучения.

Четвертым критерием станет наличие коробочной версии по, что особенно важно для учебных заведений.

Коробочные версии – это самый простой, но и самый дорогой способ приобретения Программного обеспечения разных производителей.

Коробочные версии продуктов (FPP), более всего соответствуют представлениям о том, как должен выглядеть программный продукт, благодаря тому, что покупатель сразу получает все необходимые компоненты для установки и использования продукта, а именно – лицензионное соглашение, сертификат подлинности, дистрибутив с программным продуктом, как правило, регистрационную карточку и документацию в печатном виде [4].

Коробочные версии можно приобрести у любого поставщика софта.

Последним критерием станет возможность мобильного обучения. В век цифровизации многим людям стало гораздо удобнее использовать смартфон для изучения любых материалов. Именно доступность учебного контента через мобильное устройство важно в этом пункте [5].

Далее приведем ряд популярных образовательных платформ, которые будут сравниваться:

1. Moodle – Бесплатная платформа с широкими возможностями кастомизации. Устанавливается только на свой сервер. Есть множество плагинов для расширения функционала. Требуется навыков web-разработки для администрирования.

2. iSpring – Платформа, ориентированная для корпоративного сектора. Готова к работе сразу после регистрации. Поддержка всех видов учебных материалов, вебинары, подробная статистика и редактор курсов, позволяющий быстро создать курсы и тренажеры из офисных документов и видео.

3. WebTutor – Модульная HRM-платформа, позволяющая не только выстроить обучение, но и все HR-процессы: оценку компетенции, автоматизировать подбор и первичную подготовку кадров. Сложная система с широкими возможностями.

4. Teachbase – Облачная платформа для обучения. Есть встроенный редактор курсов – страница с курсом собирается на Tilda, как обычная посадочная страница. Есть возможность продавать курсы.

5. GetCourse – Самая популярная платформа среди инфобизнесменов. Вебинары, интеграция с множеством платежных систем, защита от кражи курсов.

6. Memberlux – Плагин для WordPress, позволяющая создать учебный портал на основе обычного сайта. Единоразовая оплата, подойдет для начинающих инфобизнесменов.

По данному перечню платформ и по выявленным ранее критериям была составлена табл. 1.

Таблица 1

Сравнительная таблица платформ дистанционного обучения

Критерий	Moodle	iSpring	Teachbase	WebTutor	GetCourse	MemberLux
Создание контента	+	+	+	+	+	—
Продажа курсов	+	—	+	—	+	+
Мобильное обучение	+	+	+	+	+	+
Геймификация	+	+	—	+	+	—
Коробочная версия	+	+	—	+	—	+

Список литературы

- [1]. Андреев А.А. Введение в дистанционное обучение: учебно-методическое пособие. – М.: ВУ, 1997.
- [2]. Иванченко Д.А. Системный анализ дистанционного обучения : монография. – М.: Союз, 2005. – 192 с.

[3]. *Хусяинов Т.М.* Основные характеристики массовых открытых онлайн-курсов (МООС) как образовательной технологии // Наука. Мысль. – 2015. – № 2. – С. 21-29.

[4]. *Хуторской А.В.* Дистанционное обучение и его технологии // Компьютерра. – 2002. – № 36. – С. 26-30.

[5]. *Хуторской А.В.* Научно-практические предпосылки дистанционной педагогики // Открытое образование. – 2001. – № 2. – С.30-35.

Пильщиков Никита Алексеевич – студент, «Центр современного образования» Калужской области. E-mail: pilshikov.Nick97@yandex.ru

Дерюгина Елена Олеговна – доцент кафедры «Информационные системы и сети», канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: DeruginaEO@yandex.ru

Чухраев Игорь Владимирович – заведующий кафедрой «Информационные системы и сети», канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: chukhraev@bmstu-kaluga.ru

ХАРАКТЕРИСТИКА И СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЯЗЫКА ПРОГРАММИРОВАНИЯ GOLANG

Go (также Golang) – компилируемый язык программирования, разработанный в компании Google и официально представленный в 2009 году. Он предназначен для создания высокоэффективных программ, рассчитанных на многоядерные и многопроцессорные компьютеры. Golang от Google – прост, универсален и эффективен. Согласно опросу stackoverflow, язык входит в тройку наиболее востребованных в 2020 году [1].

Вместе с Google язык Go используют такие компании, как Uber, Fabric, Sendgrid, Medium, Dropbox, Netflix, Cloudflare, AmericanExpress, Salesforce, IBM, Target, Twitch, Twitter, Uber и Docker, а также российские Mail.ru Group, Tinkoff, Avito и Ozon.

Go – это универсальный язык, пригодный для любых задач. С момента анонсирования язык немного изменился, но цели и задачи у него остались прежние: этот язык предназначен для системного программирования и имеет много общих черт с языком C++ (для успешного освоения необходимы соответствующие определенные знания). При этом, по наблюдениям рынка труда, в основном на Go переходят с PHP или с Python.

С помощью механизмов многопоточности Go упрощает распределение вычислений и сетевого взаимодействия, а современные типы данных открывают программисту мир гибкого и модульного кода. Программа быстро компилируется, при этом есть сборщик мусора и поддерживается рефлексия. Размер программ на Go начинается с 3 строк и может достигать нескольких миллионов, записанных в один или несколько файлов с расширением «.go». Современные текстовые редакторы, например, Vim и Neovim, поддерживают его синтаксис [2].

Рассмотрим ряд основных особенностей языка программирования GoLang:

- Простой и понятный синтаксис. Go – язык с сильной статической типизацией и явным приведением типов, его синтаксис необременителен. Всё благодаря нетипизированным числовым константам и определению типа по присвоенному значению;

- Скорость и компиляция. Код на Go компилируется напрямую в машинный код, который зависит от используемой ОС (Linux/Windows/Mac) и архитектуры CPU машины (x86, x86-64, ARM и т. д.), на которой производится компиляция. Поэтому Go-программы работают действительно очень быстро. Весь проект компилируется в один бинарный файл, без зависимостей.

- Статическая типизация. Go является языком со статической типизацией. Это значит, что уже на этапе компиляции необходимо объявить типы всех переменных, аргументов функций и возвращаемых значений, что позволяет

избежать ошибок, допущенных по невнимательности, упрощает чтение и понимание кода, делает код однозначным;

- Отход от ООП. В языке нет классов, но есть структуры данных с методами. Наследование заменяется механизмом встраивания. Существуют интерфейсы, которые не нужно явно имплементировать, а лишь достаточно реализовать методы интерфейса;

- Богатая стандартная библиотека. В языке есть все необходимое для веб-разработки и не только. Количество сторонних библиотек постоянно растёт. Кроме того, есть возможность использовать библиотеки C и C++;

- Документация. Документация к языку Go генерируется автоматически и содержит примеры, которые можно запускать прямо на странице справки. Интерфейсы минималистичны и не требуют долгого изучения.

- Переносимость. Поскольку программа компилируется напрямую в машинный код, бинарные файлы являются переносимыми в рамках одной операционной системы и архитектуры [3].

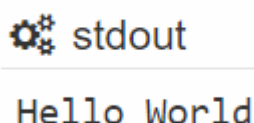
Вышеизложенные особенности делают Golang отличным от других языком, а программирование на Go – предельно простым.

Программа в Go разделяется на пакеты (package), что указывается в начале каждого файла. Имя пакета должно соответствовать директории, в которой находятся файлы, входящие в пакет. Также должен быть главный пакет main с функцией main().

Рассмотрим примертекста программы на языке GoLang, представленный на рис. 1, который будет понятен любому программисту, знакомому с синтаксисом C. Результат работы программы показан на рис. 2.

```
1 | package main
2 |
3 | import "fmt"
4 |
5 | func main() {
6 |     fmt.Println("Hello World")
7 | }
```

Рис. 1. Листинг простейшей программы на языке GoLang



```
stdout
Hello World
```

Рис. 2.Результат работы программы

Рассмотрим пример с небольшим распараллеливанием (lowconcurrency). Прогоним 2000 итераций с 300 одновременными запросами и применением только одного хеширования к каждому запросу (N = 1):

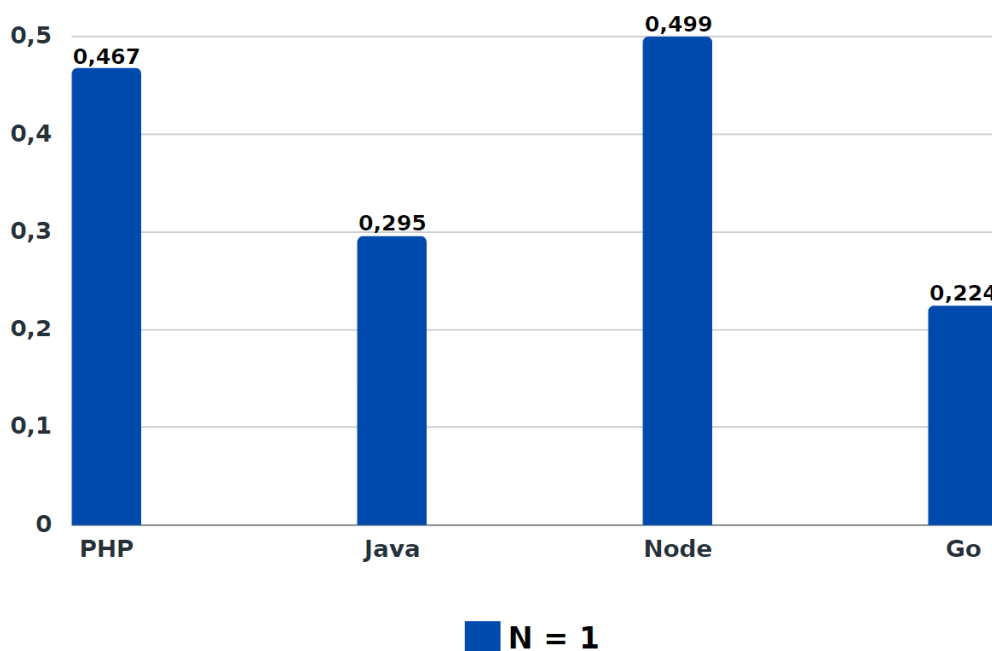


Рис. 3. Гистограмма продолжительности выполнения запросов

На основании гистограммы, показанной на рисунке 3, можно сделать вывод, что язык Go является самым быстрым из представленных, ему потребовалось наименьшее количество времени на выполнение одновременных запросов.

Программирование на Go может стать будущим разработки. Язык программирования GoLang обеспечивает высокую производительность, суперэффективную обработку параллелизма. Это молодой язык, который набрал популярность за относительно короткий период времени.

Список литературы

- [1]. *Go* (язык программирования). – [Электронный ресурс]: Режим доступа: [https://ru.bmstu.wiki/Go_\(язык_программирования\)](https://ru.bmstu.wiki/Go_(язык_программирования))
- [2] *Программирование на языке Go*. – [Электронный ресурс]: Режим доступа: <https://nedocs.ru/programmirovanie/programmirovanie-na-yazyke-go.html>
- [3] *Официальный сайт GoLang*. – [Электронный ресурс]: Режим доступа: <https://golang.org/>

Колосов Максим Игоревич – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: mgtumax@yandex.ru

Чухраев Игорь Владимирович – заведующий кафедрой «Информационные системы и сети», канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: chukhraev@bmstu-kaluga.ru

СЕКЦИЯ 14.

ИННОВАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ И НАУЧНО- МЕТОДИЧЕСКИЕ ВОПРОСЫ ВНЕДРЕНИЯ РЕЗУЛЬТАТОВ НИР В УЧЕБНЫЙ ПРОЦЕСС

ИСПОЛЬЗОВАНИЕ UNITY ДЛЯ РАЗРАБОТКИ ПРИЛОЖЕНИЙ ВИРТУАЛЬНОЙ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

Виртуальная реальность (VR) – это компьютерное моделирование 3D-среды, которая воспринимается человеком как реальная, благодаря воздействию на его органы чувств (зрение, слух, осязание). Для этого необходимо наличие устройства вывода (например, очков виртуальной реальности), а также устройства ручного управления или датчиков движения [1].

Дополненная реальность (AR) представляет собой наложение генерируемых компьютером изображений (CGI) на отображение реальности [1]. Устройством отображения дополненной реальности может служить смартфон или планшет, а также специальная AR-гарнитура.

Широкое использование виртуальной и дополненной реальности началось с выпуска игр, но эти технологии могут применяться и в других сферах. С помощью VR можно посещать достопримечательности, находящиеся в любом городе на планете не пересекая границ и даже вообще не выходя из дома, что стало особенно актуально в связи с обстановкой в реальном мире. Инженеры и конструкторы могут оценить характеристики продукта, а также симитировать различные сценарии взаимодействия с ним без затрат на производство образца, благодаря новым версиям 3DSMAX, MAYA и SolidWorks [2, 3]. Виртуальная реальность может помочь и в обучении студентов, особенно в случаях, когда реальное проведение практического занятия дорогостояще или опасно, например, при обучении проведению хирургических операций.

Unity представляет собой профессиональный игровой движок, который используется в создании видеоигр для различных платформ [4]. Unity имеет межплатформенную поддержку, которая подразумевает возможность развертывания на различных устройствах: на персональном компьютере, в Интернете, на мобильном устройстве или на консоли. Однако, при разработке VR- и AR- приложений на Unity приходится использовать наборы инструментов разработки, расширяющие интерфейс, предоставленные производителями VR- и AR- устройств, что приводит к тому, что сборка проекта будет работать только на этом устройстве [1].

Для того чтобы проект Unity мог работать с устройством виртуальной реальности необходимо настроить параметры сборки, указав в настройках плеера поддержку конкретного устройства виртуальной реальности.

Элементы пользовательского интерфейса для VR-приложений в Unity располагаются в пространстве виртуального мира и изменяют свое положение при изменении позиции пользователя (например, при повороте головы) с помощью встроенных в Unity методов, а их размеры и позиции вывода на экран задаются разработчиком приложения. К ним относятся информационный щиток, курсор в форме перекрестья, выноска, приборная панель игры, реагирующая на действия игрока и другие.

В VR-приложениях могут быть использованы те же встроенные физические законы, что и в обычных играх, написанных на этом движке. Наполнение сцены и скайбокс также задаются привычным способом.

Самого персонажа в VR-приложениях можно представить как камеру, прикрепленную к объекту, оснащенный контроллером персонажа, подобно тому, как это делается в приложениях-играх от первого лица. Рост пользователя должен запрашиваться, чтобы переместить камеру на реальный уровень его глаз, иначе пользователю придется ассоциировать себя с персонажем не своего роста, что может быть оправдано сюжетом, например, в игровом приложении. Избежать укачивания можно, добавив персонажу тело, которое может быть выбрано из стандартного набора Unity и добавлено дочерним элементом к объекту персонажа. После этого придется выполнить ряд действий, чтобы тело и голова были действительно взаимосвязаны как в реальной жизни (например, при повороте головы на 180 градусов тело также бы поворачивалось).

Для реализации движения могут использоваться различные подходы:

- движение в направлении взгляда, когда начало и окончание перемещения задается с помощью кивка;
- парящий диск, когда определено действие захода и схода с него;
- полет супермена, для которого нужны контроллеры положения рук;
- прикрепление крюка взглядом, когда долгий взгляд игрока на крюк заставляет персонажа вытащить веревку, закрепить её на крюке и совершить полет;
- пилот, когда используется кабина с элементами управления;
- поездка по рельсам, в которой пользователь может только осматриваться по сторонам, не влияя на маршрут передвижения по сцене;
- взгляд на цель, когда нажатие на кнопку перемещает персонажа к предмету, на который в это время был направлен взгляд игрока [1].

Список литературы

[1] *Линовес Дж.* Виртуальная реальность в Unity. – М.: ДМКПресс, 2016. – 360 с.

[2] *Обзор* иммерсивной среды [Электронный ресурс]. – Режим доступа: <https://www.autodesk.ru/solutions/virtual-reality>

[3] *Новые* возможности SolidWorks 2020 [Электронный ресурс]. – Режим доступа: <https://www.solidworks.com/ru/media/whats-new-solidworks-2020-edrawings-vr>

[4] *Хокинг Дж.* Unity в действии. Мультиплатформенная разработка на C# – СПб.: Питер, 2016. – 336 с.

Беккель Людмила Сергеевна – ст. преподаватель кафедры «Инженерная графика» КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: milla2606@rambler.ru

МОТИВАЦИЯ СТУДЕНТОВ НА ЗАНЯТИЯХ ПО ИНЖЕНЕРНОЙ ГРАФИКЕ

Современное профессиональное образование нуждается в новом типе преподавателя – обладающем современными методами и технологиями образования, приемами психолого-педагогической технологии, способами самостоятельного конструирования педагогического процесса в условиях конкретной практической деятельности. Другими словами занятие должно быть инновационным.

Если говорить про инженерную графику, то развитие вычислительной техники позволило создать системы автоматизации графических работ и решения геометро-графических задач. Создаются специализированные для различных отраслей промышленности автоматизированные рабочие места конструктора.

И в учебный процесс развитие цифровых технологий вносит существенные нововведения.

Инновация – это внедрённое новшество, обеспечивающее качественный рост эффективности процессов или конечных результатов. Инновация является конечным продуктом интеллектуальной деятельности человека, его фантазии, творческого процесса, изобретений и рационализации. Под инновацией следует понимать не всякое новшество или нововведение, а только то, которое серьёзно повышает эффективность действующей системы.

Технологический аспект инноваций предполагает использование различных технических средств и оборудования в обучении (компьютерные технологии, сеть Интернет). Инновационные технологии в образовании характеризуются достижением следующих эффектов:

- усвоение за минимальный промежуток времени максимального объема информации;
- повышение творческой активности обучающихся;
- овладением широким спектром практических навыков и умений.

Использование ИКТ (информационные-коммуникационные технологии) в процессе изучения курса черчения это - развитие личности обучаемого, подготовка к самостоятельной продуктивной деятельности в условиях информационного общества; развитие творческих способностей при использовании современного программного обеспечения для решения познавательных задач и формирования операционного мышления, направленного на совершенствование навыков работы на компьютере; развитие коммуникативных способностей и навыков исследовательской деятельности.

Формы использования ИКТ:

1. Использование готовых электронных продуктов;
2. Использование мультимедийных презентаций;

3. Использование ресурсов сети Интернет;
4. Использование интерактивной доски;
5. Использование программы «Компас 3D LT», «AutoCAD».

Использование готовых электронных продуктов, мультимедийных презентаций, ресурсов сети Интернет – это использование иллюстрационного наглядного материала: видеofilьмов, слайдов, слайд-фильмов, слайд-презентаций.

Инженерная графика – одна из немногих учебных дисциплин, которая идеально укладывается в компьютерные технологии и активно используется в преподавании данного предмета. Повышение эффективности обучения черчению во многом зависит от использования на уроках дидактических материалов, дидактических игр и компьютерных технологий. Используя информационные технологии при изучении черчения активизируется процесс обучения, формируются навыки работы с компьютером, экономится времени урока, появляется возможность увеличения объема нового материала на уроке и сокращение времени на его объяснение, сокращается время на подготовку к уроку, создается возможность выполнения виртуальных демонстрационных показов с использованием недоступного оборудования. Для подготовки к уроку черчения, используется программа PowerPoint.

Использование презентаций открывает более широкие возможности для творческого преподавания, как черчения, так и других предметов. Презентации, как наглядные пособия, помогают преподавателю излагать учебный материал, развивают навыки наблюдения и анализ формы предметов, обеспечивают прочное усвоение обучающимися знаний, повышают интерес к предмету.

Использование информационных технологий в учебном процессе обеспечивает реализацию интенсивных форм и методов обучения, организацию самостоятельной учебной деятельности, способствует повышению мотивации обучения за счет возможности использования современных средств комплексного представления и манипулирования аудиовизуальной информацией, повышения уровня эмоционального восприятия информации.

Основной целью образования становится не простая совокупность знаний, умений и навыков, а основанная на них личная, социальная и профессиональная компетентность – умение самостоятельно добывать, анализировать и эффективно использовать информацию, умение и рационально жить и работать в быстро изменяющемся мире. Преподаватель является главным действующим лицом любых учебных преобразований, которые требуют от него повышения своего профессионального мастерства. В настоящее время утверждение о том, что педагогическая деятельность является по своей природе творческой, стало общепринятым. «Творчество - это деятельность, порождающая нечто новое на основе реорганизации имеющегося опыта и формирования новых комбинаций знаний, умений, продуктов».

Результатом творчества является введение в педагогический процесс инноваций. В том числе: открытие, утверждающие идеи, способные преобразовывать педагогическую действительность; изобретения, разработка и внедрение новых элементов педагогических технологий; педагогическое рационализаторство – усовершенствования, связанные с модернизацией и адаптацией к конкретным условиям уже использования методов и средств воспитания и обучения.

Эффективность внедрения инноваций зависит от целого ряда факторов: от особенностей предлагаемого новшества, от потенциала учебного заведения, от позиции и квалификации администрации и инициаторов инновационной работы. Главной преградой для внедрения инноваций служит качественное состояние, уровень профессионализма педагогического состава организации образования. Например, новые технологии обучения требуют от преподавателя (помимо от профессиональной компетентности в своей предметной области) педагогического мастерства. Если урок современный, то он обязательно закладывает основания для будущего. Как бы новации не вводились сегодня, призывая нас перейти к нетрадиционному уроку, только на уроке, как сотни и тысячи лет назад, встречаются участники образовательного процесса: преподаватель и студент. Что бы ни твердили о компьютеризации и дистанционном образовании, преподаватель всегда будет главным лицом в обучении. За ним – знания, опыт, понимание и применение этих знаний.

Для преподавателей специальных дисциплин необходимо обладать предметно-углубленной ИКТ-компетентностью, соответствующей осознанному методически грамотному использованию ИКТ в преподавании своего предмета. Для того чтобы преподаватели специальных дисциплин имели волю и желание к внедрению информационных и коммуникационных технологий в образовательный процесс, желание повышать свою информационно-коммуникационную культуру возникает необходимость создания образовательной среды, насыщенной аппаратными и программными средствами информационно-коммуникационных технологий. Возможности этой среды должны использоваться преподавателями специальных дисциплин для развития у студентов информационной компетентности и информационной культуры, для собственного профессионального развития. Это важно, так как информационная компетентность обучаемых является одной из ключевых компетентностей, которые призвано формировать образовательное учреждение.

Использование современных технологий позволяет преподавателям, как осваивать современные стратегии и приемы организации работы с образовательной информацией, так и развивать собственную информационную культуру.

Современный преподаватель должен использовать всё лучшее из традиционных технологий, находить инновационный подход к учебному процессу, всегда быть ориентированным на уникальную неповторимость

каждого ученика, на развитие его индивидуальных способностей и прежде всего на повышение качества образования. Творчество преподавателя и студента безгранично. Важно только умело направить его для достижения поставленных учебных целей – подготовки высококвалифицированного специалиста.

На практике можно заметить, что инновационные методы обучения дают возможность качественно и быстрее получить хороший результат. Применение разнообразных инновационных методов, повышает у обучающихся интерес к самой учебно-познавательной деятельности, повышает мотивацию и в купе решает комплекс воспитательных, обучающих, поставленных задач.

Создавать новое – это и есть инновация.

Список литературы

[1]. *А.А. Чекмарев*. Начертательная геометрия и черчение. – М.: Гуманитарный издательский центр ВЛАДОС, 1999. – С. 4

Сахаров Владимир Валентинович – старший преподаватель КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: vlad.saharov2011@yandex.ru

РЕОРГАНИЗАЦИЯ КУРСА ДИСЦИПЛИНЫ НАЧЕРТАТЕЛЬНАЯ ГЕОМЕТРИЯ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Начертательная геометрия является общепрофессиональной дисциплиной и служит базой для изучения инженерной и компьютерной графики в технических ВУЗах.

Успеваемость по дисциплине в последние годы обучения значительно снизилась (70% обучающихся могут сдать экзамен с первого раза), значительно увеличилось количество оценок «удовлетворительно» из общего числа студентов, успешно сдавших экзамен.

По мнению авторов, неуспеваемость и низкое качество знаний обусловлены не только личностными качествами обучающегося (психологические и интеллектуальные факторы успешности обучения, интересы, воля, самооценка и т.д.), но и объективными факторами:

- несоответствие школьной геометро-графической подготовки требованиям к предшествующей подготовке и знаниям: отсутствие курса черчения в школах, недостаточные навыки работы с традиционными чертежными инструментами у студентов;

- сокращение аудиторных часов на изучение дисциплины: при составлении учебной программы согласно действующим стандартам большее количество часов выделено на самостоятельную работу обучающихся;

- отсутствие интереса к дисциплине у обучающихся: отсутствие осознанного понимания студентами окончательной цели и задач при изучении дисциплины, её применения в последующем обучении;

- недостаточный уровень развития пространственного мышления у студентов.

При обучении возникают проблемы связанные прежде всего с пониманием и реализацией алгоритмов решения графических задач, студенты, запоминая определенные этапы решения (методом заучивания), не умеют решать оригинальные задачи. Например, задачи, где фигура занимает частное положение относительно основных плоскостей проекций.

Начертательная геометрия как наука основана на методе проецирования геометрических фигур на совмещенные плоскости проекций, содержит ряд алгоритмов, реализация которых позволяет построить изображения (проекции) геометрических фигур на плоскостях, изучить свойства фигур (точки, линии, поверхности), определить их метрические и позиционные характеристики [1]. Эти задачи посредством математического моделирования в САД-системах реализуются, безусловно, с большей точностью в автоматизированном режиме проектирования.

Пока существует чертеж «в чистом виде» (в стандартах ЕСКД, на производстве), как средство передачи технической информации об изделии, начертательная геометрия необходима как «азбука создания чертежа».

По мнению авторов, совершенствование учебно-методического комплекса и содержания рабочей программы дисциплины должно быть реализовано посредством решения следующих задач:

- обеспечение четкой междисциплинарной взаимосвязи с аналитической геометрией, параллельного изучения графических и аналитических алгоритмов решения геометрических задач;

- реорганизация курса дисциплины инженерная графика для параллельного изучения начертательной геометрии и поверхностного моделирования в САД-системах в инженерной графике;

- создание и внедрение мультимедийных курсов, лекций, презентаций по дисциплине;

- применение в качестве «чертежного инструмента» компьютерных графических программ, как двухмерного аппарата создания проекций.

Как следствие возникает необходимость совершенствования учебного процесса по начертательной геометрии, направленное на актуализацию содержания курса дисциплины, который обеспечит большую преемственность обучения в параллельно изучаемых и последующих дисциплинах и позволит обучающимся использовать полученные знания для решения проектных графических задач в инженерной графике и других инженерно-графических дисциплинах.

Список литературы

[1] *Фролов С. А.* Начертательная геометрия: Учебник / Фролов С.А., – 3-е изд., перераб. и доп. – М.: НИЦ ИНФРА-М, 2019. – 285 с.: – (Высшее образование: Бакалавриат). – ISBN 978-5-16-010480-5.

Сулина Ольга Владимировна – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: sulina.olga@yandex.ru

Шестернина Елена Анатольевна – старший преподаватель КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: elena13elen@yandex.ru

РОЛЬ ИНЖЕНЕРНО-ГРАФИЧЕСКИХ ДИСЦИПЛИН В ПОДГОТОВКЕ БАКАЛАВРОВ ПО НАПРАВЛЕНИЮ ИННОВАТИКА

В современных условиях главной целью образования в техническом вузе является подготовка незаменимых специалистов, обладающих высоким уровнем профессиональной квалификации, компетентностью в избранном деле и комплексом личностных качеств, актуальных в современных условиях информатизации профессиональной деятельности и представляющих социальную значимость и ценностную потребность для вступающего в трудовую жизнь молодого человека. Чем выше уровень развития профессионально и личностно важных качеств у студентов, тем эффективнее и качественнее их профессиональная подготовка. Современная компьютеризированная графическая подготовка в техническом вузе - это фундаментальная сфера знаний, умений и специфических личностных качеств, без которых не может состояться современный инженер. В значительной степени возросла потребность в специалистах, способных к проявлению творчества в решении новых инженерно-геометрических задач. Это предопределило новый интерес к проблеме формирования творческой личности специалиста.

К качественной графической подготовке будущих специалистов относится развитое пространственное мышление, знание правил оформления конструкторской и технологической документации в соответствии с ГОСТами ЕСКД, владение ручными и автоматизированными методами изображения пространственных форм и умение применять их в решении инженерных задач.

В последние годы заметно расширился круг задач, решаемых методами начертательной геометрии, инженерной и компьютерной графики, и, как следствие, возросла значимость графических дисциплин в инженерном образовании. Графические изображения являются одним из главных средств познания окружающего мира, инструментом творческого и пространственного мышления личности. Инженерная графическая подготовка дает возможность будущим специалистам оперировать понятиями и пространственными образами, связанными с визуализацией информации, транслировать её с помощью графических средств.

В соответствии с новым ФГОС ВПО, высокое качество графической подготовки инженера машиностроительной промышленности призвана обеспечить преподаваемые в вузе дисциплины, входящие в состав профессионального цикла: начертательная геометрия, инженерная и компьютерная графика. Целью изучения данных дисциплин является приобретение студентами знаний теоретических основ построения и преобразования проекционного чертежа как графической модели пространственных фигур с последующим применением навыков в практике выполнения технических чертежей, их оформления

по правилам государственных стандартов, в том числе с использованием компьютерной техники.

В непосредственном взаимодействии дисциплины начертательная геометрия, инженерная и компьютерная графика способствуют развитию пространственного представления и воображения, конструктивного и творческого мышления, а также воспитанию профессиональной и графической культуры и грамотности.

Учебные курсы «Начертательная геометрия» и «Инженерная графика» являются классическими в подготовке будущих инженеров. Эти дисциплины должны обеспечивать студента технического вуза фундаментальными геометро-графическими знаниями и умениями, на базе которых будущий бакалавр сможет успешно изучать такие дисциплины, как теория машин и механизмов, сопротивление материалов и другие конструкторско-технологические и специальные дисциплины, а также овладевать алгоритмическими навыками решения геометрических задач геометрического моделирования.

Задача начертательной геометрии сводится к изучению способов получения определенных графических моделей, основанных на ортогональном проектировании, и умению представлять пространственные формы и их взаимоотношения. Инженерная графика – общеинженерная учебная дисциплина, обучающая студентов умениям и навыкам изложения технических идей с помощью чертежа, а также пониманию по чертежу принципа действия изображаемого технического изделия.

В образовательном процессе формируется репродуктивное и продуктивное воображение, необходимое для дальнейшей профессиональной деятельности. Формирование необходимых профессионально значимых инженерных умений и навыков студентов является первоочередной задачей изучения графических дисциплин.

В процессе выполнения графических работ вырабатываются чертежные навыки, умения владеть приспособлениями и инструментами, глазомер, развивается пространственное воображение. К основным видам графических работ относятся различные чертежи, эскизы, технические рисунки, графики, диаграммы, планы, схемы.

Конструкторско-технологическая компетентность специалиста инноватика предполагает уровень осознанного применения графических знаний, умений и навыков, опирающийся на знания функциональных и конструктивных особенностей технических объектов, опыт графической профессионально-ориентированной деятельности, свободную ориентацию в среде графических инф. технологий.

Список литературы

[1]. *Кальницкий В.Л., Тарасов Б.Ф.* Введение в машинную графику. – Л., 1986. – 94 с.

[2]. *Федеральный* государственный образовательный стандарт высшего профессионального образования по направлению подготовки 131000 Инноватика – введ. 28.10.2009. – М., 2009. – 31 с.

[3]. *Федеральный* государственный образовательный стандарт высшего профессионального образования по направлению подготовки 151000 Технологические машины и оборудование – введ. 09.11.2009. – М., 2009. – 28 с.

[4]. *Чопова Н.В.* Формирование профессиональных качеств будущего специалиста при обучении инженерной графике в вузе// Вестник ЦМО МГУ. – 2009. – №3. – С. 96-101.

Сломинская Елена Николаевна – зав. кафедрой «Инструментальная техника и инженерная графика», канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: slominskaya_elen@mail.ru

Аксенов Артем Дмитриевич – студент МК8-71 КФ МГТУ им. Баумана. E-mail: artemic@cloud.com

САМОСТОЯТЕЛЬНАЯ РАБОТА КАК МЕТОДИЧЕСКАЯ ОСНОВА САМООБРАЗОВАНИЯ ОБУЧАЮЩИХСЯ В КОНТЕКСТЕ НЕПРЕРЫВНОГО ОБРАЗОВАНИЯ

В статье рассматриваются вопросы организации и методического сопровождения самостоятельной работы обучающихся в контексте непрерывного образования. Акцент делается на формирование готовности к самообразованию – как одной из форм самостоятельной работы обучающихся на каждом этапе образования.

На современном этапе развития обществу требуются специалисты, обладающие помимо профессиональной компетентности, еще и компетенцией в сфере самообразования. Самостоятельность в принятии решений в ситуации выбора, ответственность, профессиональная и информационная мобильность, познавательная и творческая активность и самостоятельность – вот далеко не полный перечень качеств, обеспечивающих самообразовательную компетенцию и позволяющих специалисту быть конкурентоспособным на рынке труда. Рассматривая педагогические аспекты этого вопроса, можно говорить о том, что самообразование это самостоятельная развивающе-образовательная деятельность обучающихся по постановке цели, осознания мотивации, выбору средств и методов работы, контролю и рефлексии результатов - при некоторой управляющей функции обучающего.

Очевидно, что процесс формирования готовности к самообразованию должен охватывать все ступени образования – начиная со школы, и заканчивая профессиональным образованием. Так как формирование готовности к самообразованию сугубо индивидуальный процесс, на который оказывают влияние возрастные и личностные особенности обучающихся, поэтому на каждом этапе должны использоваться соответствующие психолого-педагогические методы сопровождения и самообразовательные технологии. В свете этого коротко коснемся школьного этапа и более подробно остановимся на профессиональном образовании.

На этапе начальной школы психологической обусловленностью рассматриваемого процесса являются широкие познавательные потребности ребенка, в процессе удовлетворения которых возможно осуществлять целенаправленное формирование начальной готовности к самообразованию. Это включает в себя присвоение ребенком начальных знаний о ценности самообразования, о своих собственных познавательных интересах, формирование умений поиска информации в библиотеке – библиотечно-библиографические знания (ББЗ), отбора и представления необходимой информации, *самостоятельной целевой рациональной организации самостоятельной работы* и т.д. Целевой такая самостоятельная работа является потому, что цель этой деятельности ребенок старается ставить самостоятельно, в зависимости от предполагаемого результата. А рациональной самостоятельная работа становится тогда, когда осоз-

нанно выбираются способы работы, необходимые для достижения результата. На этом этапе образования закладываются основы рефлексивной деятельности младших школьников, особенно продуктивно формируемые в ходе самообразовательной проектной деятельности. Таким образом, по окончании четвертого класса ребенок обладает начальной суммой знаний о важности самообразования, у него заложены основы информационной культуры самообразования и сформированы начальные умения субъектной самообразовательной деятельности.

Основной задачей средней школы является совершенствование способов самообразования. Учитывая возрастные и психологические особенности подростков и старших школьников, организаторы самообразовательного процесса (учителя, библиотекари, психологи, родители, администрация школы) предоставляют им возможность реализовать (сформировать) свою субъектность в самообразовательной деятельности в сфере самопознания (5 класс), группового самообразования (6,7 класс), развития личностных и профессионально значимых качеств (8,9 класс). Параллельно с этим происходит дальнейшее непрерывное развитие информационной культуры самообразования школьника. На этапе средней школы, на базе ББЗ, полученных ранее, формируются умения работы с цифровыми образовательными ресурсами (ЦОБР) и информационно-коммуникационными технологиями (ИКТ), медиаресурсами. Самообразовательный вектор в 9-10 классах ориентирован на вопросы профессионального самообразования. *Самостоятельная работа*, не переставая быть целевой и рациональной, призвана на этом этапе помочь школьнику развить свои личностные качества, она *преобразуется в познавательную самостоятельность* – весьма ценное качество, востребованное в любой предметной области.

Таким образом, к моменту поступления в профессиональное образовательное учреждение любого уровня, обучающийся обладает знанием о ценности самообразования и профессионального самообразования, совокупностью способов самообразования (субъектного, группового), а также информационной культурой самообразования базового уровня. Помимо этого у выпускника школы сформированы необходимые для самообразовательной деятельности личностные качества: волевые (целеустремленность, инициативность, настойчивость, дисциплина); потребность и способность к самоорганизации времени и пространства; потребность и способность к самопознанию; творческая, познавательная и умственная *самостоятельность*.

Приступая к следующему, профессиональному образовательному этапу, обучающийся переходит на новую ступень формирования готовности к самообразованию. На предыдущем этапе самообразовательная деятельность носила более познавательный и учебный характер, в соответствии с ведущей учебной деятельностью школьника. Акцент ставился на приобретение и совершенствование техники субъектного и группового самообразования. Так как, начиная с возраста ранней юности (15-17 лет) изменяется тип ведущей деятельности на профессиональную учебу, то и вектор самообразования смещается в

сторону профессионального самообразования. Хотя возможно и сочетание с самообразованием в другой личностно значимой предметной области.

Еще одной отличительной чертой этого этапа являются те психологические черты, которые характерны для ранней и поздней юности (15-25 лет). Молодежи присущи дивергентное мышление, высокая творческая и мыслительная активность, интенциальность, способность к самоконтролю и саморегуляции, сформированность ценностных ориентаций. Все эти психологические особенности, базирующиеся на сформированных ранее базовых самообразовательных знаниях и умениях, позволяют более динамично осуществлять процесс формирования готовности к профессиональному самообразованию студентов. Как показывает опыт, целевая деятельность организаторов самообразовательного процесса в профессиональных учебных заведениях должна носить практико-ориентированный характер по всем изучаемым дисциплинам. Это позволяет студентам сразу включаться в самообразовательное пространство и формировать и развивать профессионально значимые личностные качества. Претерпевает изменения и *самостоятельность юношества - становится субъектно-активной, преобразующей, творческой.*

Для успешного формирования готовности к самообразованию необходимо внедрять в традиционный образовательный процесс целевые (имеющие субъектно значимую, осознанную, сформулированную цель) методики и технологии, базирующиеся на концепции личностно ориентированного обучения и воспитания. Методической основой самообразовательных методик и технологий служат целевые ситуации выбора, ситуации успеха, банк способов самообразовательной деятельности, субъектная и групповая проектная деятельность, ролевые игры, проблемные методы и т.д.

Большинство вопросов в этой статье посвящено формированию готовности к самообразованию обучающихся – школьников, студентов. Однако, возвращаясь к определению самообразования, приведенному в начале, необходимо отметить важность управляющей роли обучающихся – учителей, преподавателей, библиотекарей, психологов, родителей, администрации образовательного учреждения. Управление самообразованием заключается в грамотном психолого-педагогическом, информационном, организационном сопровождении процесса, что в свою очередь подразумевает соответствующую подготовку или переподготовку профессорско-преподавательского состава образовательных учреждений. В ходе научно-методических, обучающих, практических семинаров организаторы образовательного процесса изучают теоретические и методические, дидактические основы управления самообразованием обучающихся разных возрастных групп, вскрывают механизмы формирования готовности к самообразованию, обмениваются опытом. Необходимыми к рассмотрению на таких семинарах вопросами следует считать: теоретические аспекты процесса самообразования обучающихся; субъекты самообразовательного процесса и их инновационные функции; научные аспекты педагогики, психологии и управления самообразованием обучающихся; библиотека как совре-

менный информационно-просветительский центр самообразования. Самообразование обучающихся есть стимул для обучающихся.

Таким образом, формирование готовности к самообразованию обучающихся есть системный, полифункциональный, субъектный процесс, охватывающий все ступени образования и, становясь личностно-значимым, продолжается всю жизнь. На разных этапах этот процесс характеризуется психолого-педагогическими, информационными, организационными особенностями, учет которых делает его максимально эффективным, динамичным, взаимостимулирующим для всех его участников.

Список литературы

[1]. *Крицкая А.Р.* Формирование готовности обучающихся в профессиональном учебном заведении к самообразованию. – Калуга: Издательство научной литературы Н.Ф. Бочкаревой, 2008. – 174с.

[2]. *Крицкая А.Р.* Некоторые концептуальные основы самообразования // Вопросы философии. – 2013. – № 5. – С. 70-74.

[3]. *Калугин Ю. Е.* Профессиональное самообразование, содействие профессиональному самообразованию / Калугин Ю.Е. монография // М-во образования и науки Российской Федерации, Федеральное агентство по образованию, Южно-Уральский гос. ун-т, Каф. «Гуманитарные науки». Челябинск, 2009.

[4]. *Лобанов Н.А.* О национальной гуманитарной инициативе «профессиональное самообразование как государственно-корпоративная подсистема непрерывного профессионального образования» // Образование через всю жизнь: непрерывное образование в интересах устойчивого развития: Материалы второго этапа 13-й Международной конференции. / Под науч. ред. Л.Н. Рулиене, И.А. Маланова, Н.А. Лобанова. – 2016. – С. 26-29.

Крицкая Анна Рудольфовна – доцент, канд. пед. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: anna_kritskaya69@list.ru

Китаева Тамара Сергеевна – доцент, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: kf_MGTU_FIZ@mail.ru

СПОСОБЫ ПОСТРОЕНИЯ ЭЛЛИПСА

Эллипс представляет собой геометрической место точек, сумма расстояний от каждой из которых до двух данных точек есть (величина) постоянная.

Пусть в плоскости даны две точки F_1 и F_2 (фокусы эллипса) на расстоянии $2c$ друг от друга (рис. 1).

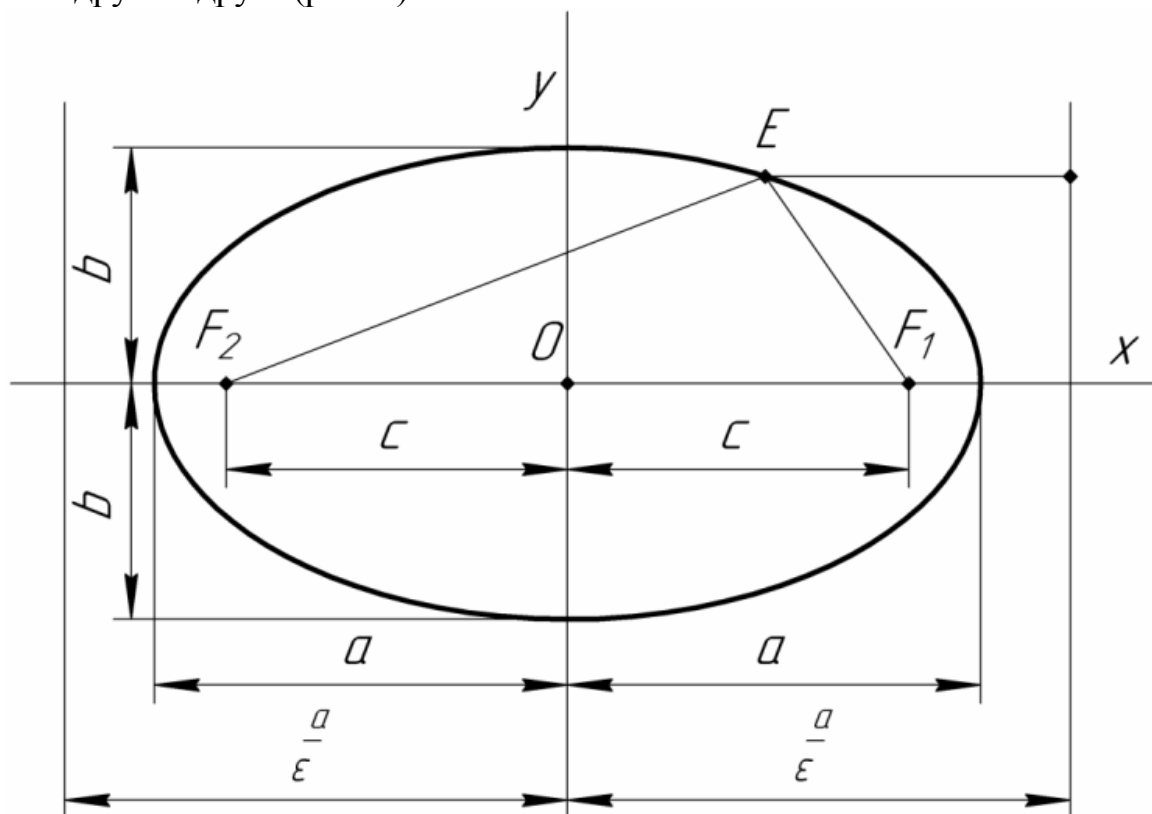


Рис.1. Построение эллипса по его параметрам

Любая точка E плоскости принадлежит эллипсу, если соблюдается условие:

$$EF_1 + EF_2 = 2a,$$

где $2a$ – данная длина.

Если фокусы F_1 и F_2 совпадают, то

$$EF_1 = EF_2 = 2a.$$

Получаем геометрическое место точек, равноудаленных от одной данной точки, т.е. окружность. Поэтому окружность есть частный вид эллипса.

Уравнение эллипса имеет следующий вид:

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1,$$

где $b^2 = a^2 - c^2$.

Такое простейшее уравнение эллипса называют коническим. Оси координат являются осями симметрии эллипса. Точку пересечения осей симметрии

называют центром эллипса; точки пересечения эллипса осями симметрии – вершинами эллипса. Отрезки, соединяющие противоположные вершины эллипса, равные $2a$ и $2b$, называют соответственно большой и малой осями эллипса.

Диаметры эллипса – отрезки прямых, проходящих через центр эллипса. Два таких диаметра, каждый из которых делит пополам хорды, параллельные другому, называют сопряженными. Большая и малая оси эллипса являются сопряженными взаимно перпендикулярными диаметрами.

Величину $\frac{2a}{2c} = \varepsilon$ – отношение фокусного расстояния к длине большой оси называют *эксцентриситетом эллипса*. Для эллипса $\varepsilon < 1$.

Две прямые, перпендикулярные к фокальной оси эллипса и удаленные от центра на величину $\frac{a}{\varepsilon}$, называют *директрисами эллипса*. Директрисы обладают следующим свойством.

Отношение расстояний от любой точки эллипса до фокуса и соответствующей директрисы есть величина постоянная, равная ε .

Укажем способ построения эллипса по точкам, исходя из его определения и канонического уравнения.

Из уравнения определяем величины a и b , подставляя их в заданном масштабе отрезками на осях координат (рис. 2.).

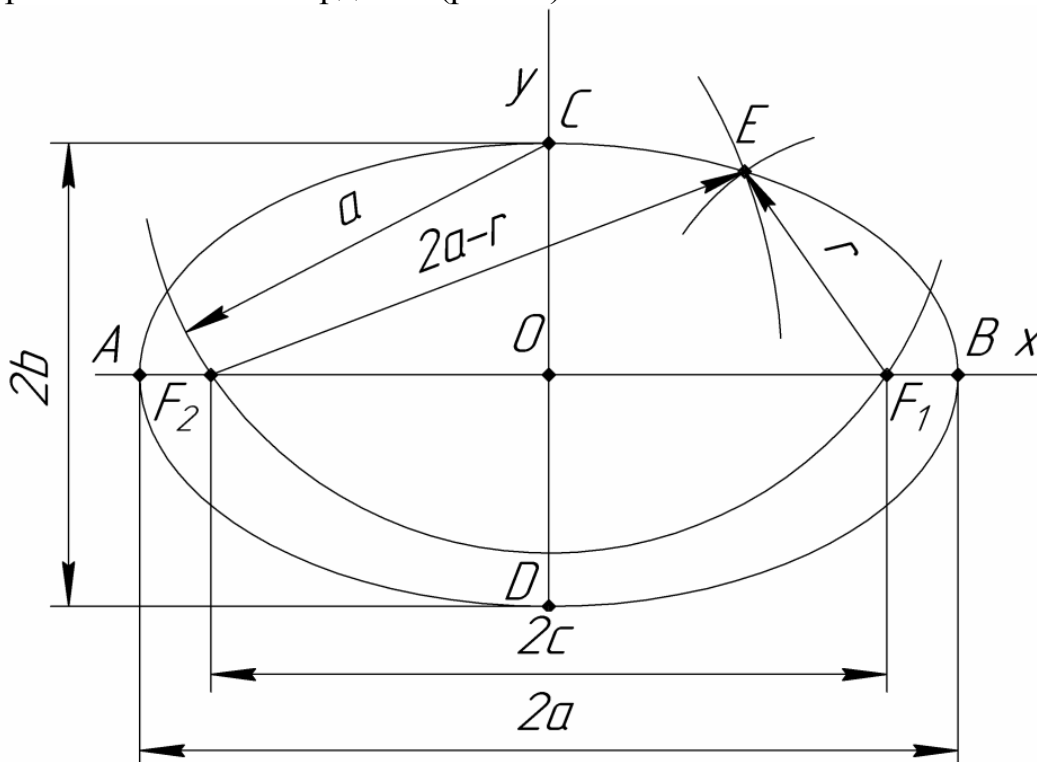


Рис. 2. Построение эллипса по его уравнению

Из точки C , как из центра, радиусом a проводим дугу, которая пересекает прямую AB в точках F_1 и F_2 . Точки F_1 и F_2 являются фокусами эллипса, так

как соблюдается зависимость $c^2 = a^2 - b^2$. Из фокусов F_1 и F_2 , как из центров проводим дуги окружностей соответственно радиусам r и $2a - r$, где r – произвольной длины. Точки пересечения окружностей являются точками эллипса, так как сумма расстояний от каждой из них до фокуса равна $2a$ и есть величина постоянная. Изменяя радиус r и повторяя построения, получаем новые точки эллипса.

При параллельном проецировании окружность проецируется на плоскость или в виде окружности (частный случай), или в виде эллипса (общий случай).

Окружность проецируется на плоскость проекций без искажения, если её плоскость параллельна плоскости проекций. Если же окружность принадлежит проецирующей плоскости, то одна проекция представляется в виде отрезка прямой, равного диаметру окружности, а другая в виде эллипса. Если окружность принадлежит плоскости произвольного положения, то ортогональными проекциями её являются эллипсы. Эллипс есть кривая, родственная окружности.

На рис.3. представлены два произвольно выбранных и делящихся пополам отрезка – A_1B_1 и C_1D_1 . Рассмотрим эти отрезки как сопряженные диаметры эллипса. Один из отрезков, например A_1B_1 , примем за диаметр окружности, родственной эллипсу. Здесь соответственные диаметры эллипса и окружности совпадают ($AB \equiv A_1B_1$).

Диаметры AB и CD родственной эллипсу окружности являются взаимно сопряженными, т.е. взаимно перпендикулярны. Построив окружность и наметив на ней ряд точек E , можем определить и соответствующий им ряд точек E_1 эллипса.

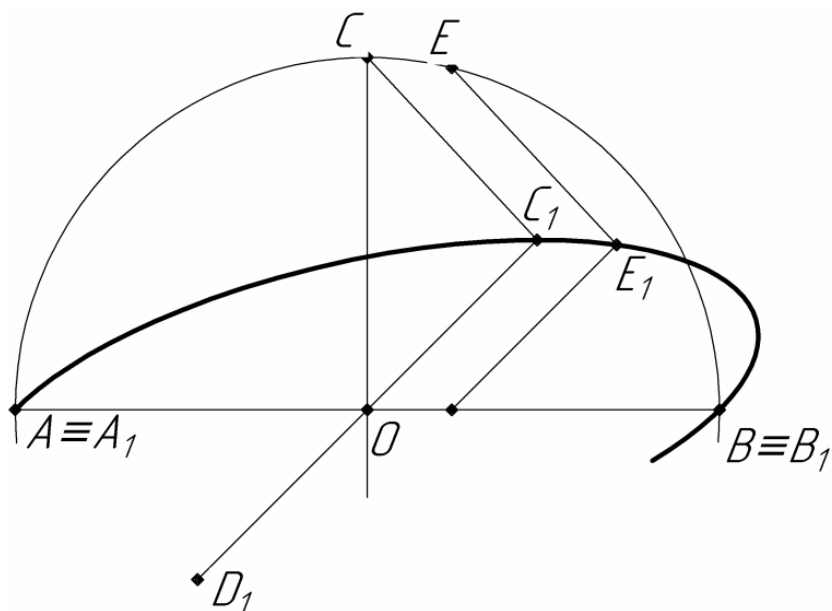


Рис. 3. Построение эллипса по двум отрезкам

Укажем другие способы построения эллипса как линии, родственной окружности, если даны два его сопряженных диаметра. Пусть сопряженным

диаметрам AB и CD окружности соответствуют сопряженные диаметры A_1B_1 и C_1D_1 родственного ей эллипса (рис. 4.). Докажем, что точке E (рис. 4, а) окружности соответствует точка E_1 эллипса (рис. 4, б). Через точку E окружности проведем прямую BE до пересечения её в точке K с прямой AC . В треугольнике ABK прямые AE , BC и KM являются его высотами. Они пересекаются в точке G .

Исходя из условия соответствия двух родственных фигур – окружности и эллипса – устанавливаем, что треугольнику ABK с его высотами AE , BC и KM соответствует треугольник $A_1B_1K_1$ с прямыми A_1E_1 , B_1C_1 и K_1M_1 . Точка E окружности соответствует E_1 эллипса.

Пусть эллипс задан сопряженными диаметрами A_1B_1 и C_1D_1 (рис. 4, б).

Точки эллипса можно определить следующими построениями. На прямой A_1C_1 намечаем произвольную точку K_1 . Через точку K_1 проводим прямую, параллельную диаметру C_1D_1 , находим точку G_1 пересечения её с прямой C_1B_1 . Точка E_1 эллипса определяется на пересечении прямых A_1G_1 и K_1B_1 . Повторяя такие построения, найдем целый ряд точек эллипса.

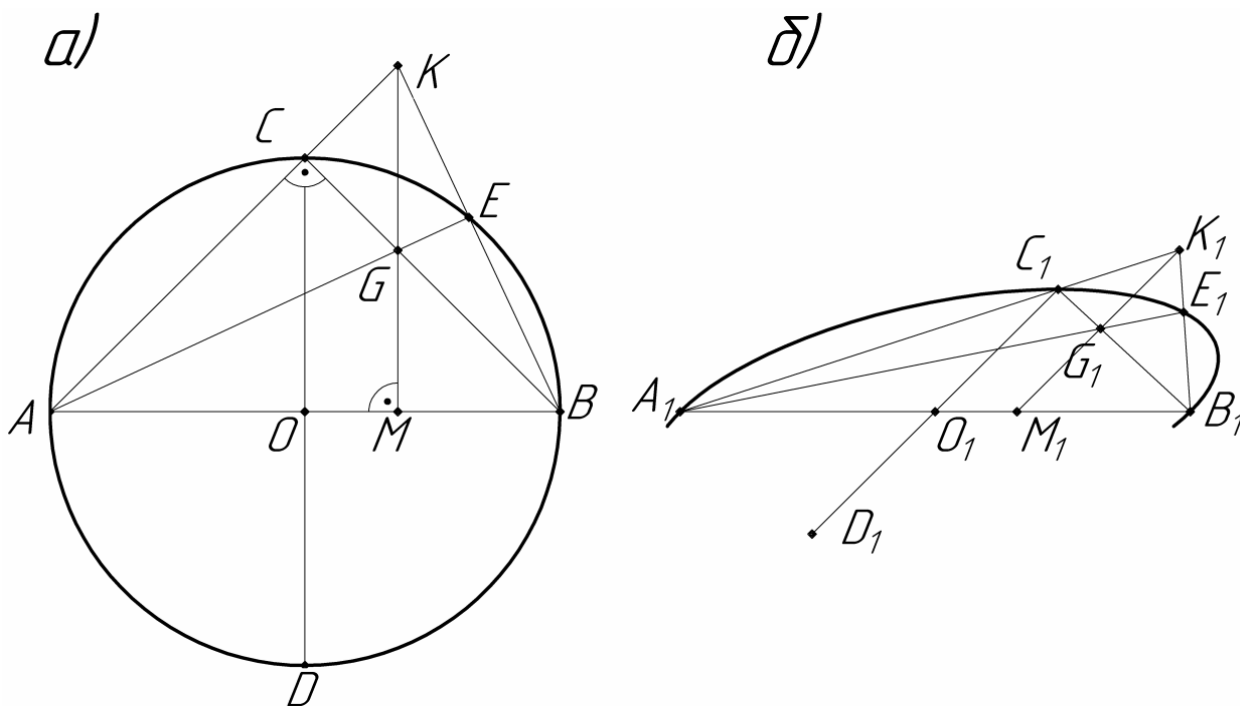


Рис.4. Построение эллипса как линии, родственной окружности

На рис.5. показан другой способ построения эллипса по его сопряженным диаметрам. На полудиаметрах O_1C_1 и O_1B_1 строим параллелограмм. Стороны параллелограмма делят соответственно на одинаковое число равных отрезков.

Лучи, проведенные из точек C_1 и B_1 концов полудиаметров через одинаково нумерованные точки сторон параллелограмма, пересекаются в точках эллипса.

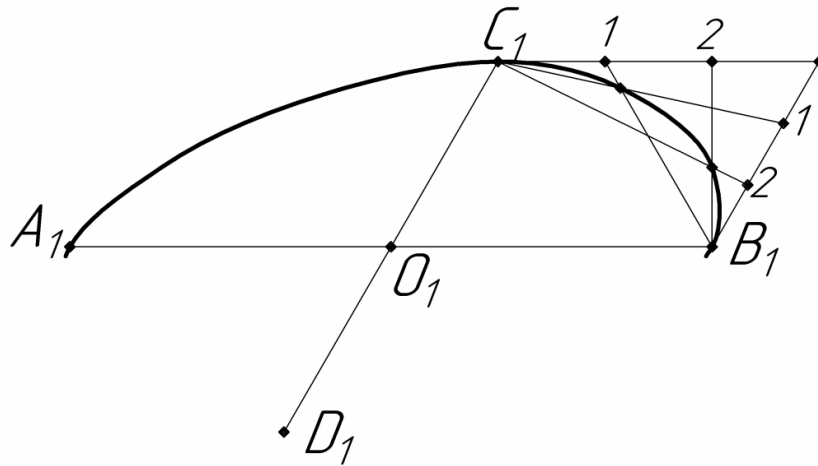


Рис.5. Построение эллипса по сопряженным диаметрам

Теорема. Ортогональной проекцией окружности, плоскость которой не перпендикулярна к плоскости проекций, является эллипс.

Большая ось эллипса равна и параллельна тому диаметру окружности, которому параллельна плоскость проекции.

Малая ось эллипса параллельна проекции направления плоскости окружности и равна проекции диаметра окружности, являющегося линией наибольшего ската плоскости этой окружности.

На рис.6. показан способ построения эллипса по заданным его осям. Он основан на параллельном проецировании окружности. Для построения точек эллипса из центра O проводим две окружности, диаметрами которых являются большая и малая оси эллипса. Из центра O окружностей произвольно проводим луч и помечаем точки E и K пересечения его с окружностями. Из точек E и K проводим прямые, параллельные соответственно осям A_1B_1 и C_1D_1 эллипса. Точка K_1 их пересечения является точкой эллипса, что легко доказать.

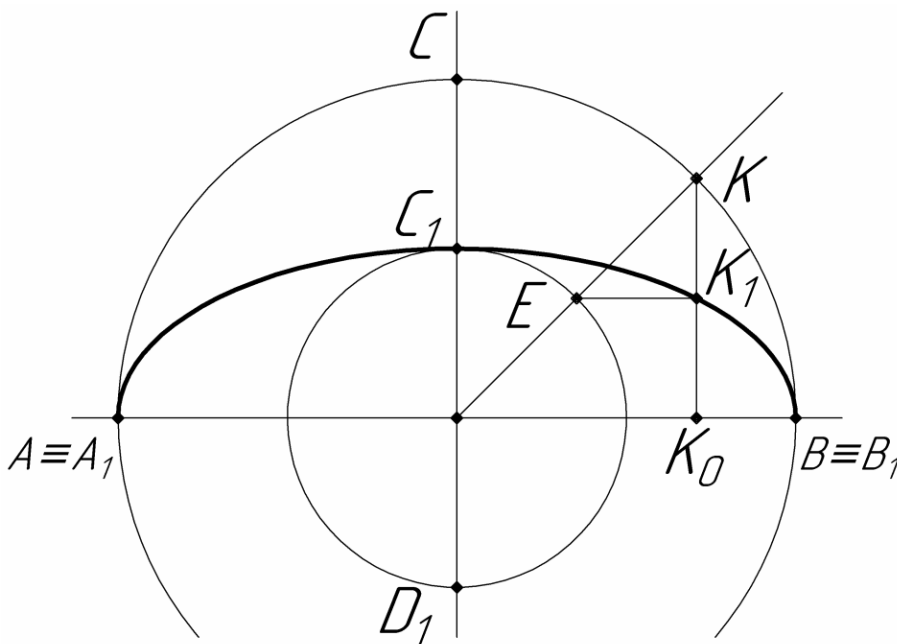


Рис. 6. Построение эллипса по его осям

Рассмотрим треугольник OKK_0 .

Здесь

$$OK = \frac{A_1B_1}{2}, OE = \frac{C_1D_1}{2}, EK_1 \parallel OK_1.$$

Очевидно

$$\frac{K_1K_0}{KK_1} = \frac{OE}{OK} = \frac{C_1D_1}{A_1B_1} = const.$$

Выбирая другие лучи и помечая точки на окружностях, построим ряд соответствующих точек эллипса.

На рис.7. пересекающиеся в точке O отрезки KU и GE являются сопряженными диаметрами эллипса. Один из полу диаметров, например OK , повернем на 90° вокруг центра O по часовой стрелке. Получим отрезок OK_1 . Через точки K_1 и E проводим прямую из середины S отрезка K_1E , как из центра, описываем дугу радиусом OS . Прямая K_1E пересекает дугу окружности в точках M и N . Отрезок MN определяет сумму полуосей эллипса.

Прямые OM и ON указывают направление малой и большой полуосей эллипса, а величины этих полуосей соответственно равны отрезкам $EN = b$ и $EM = a$.

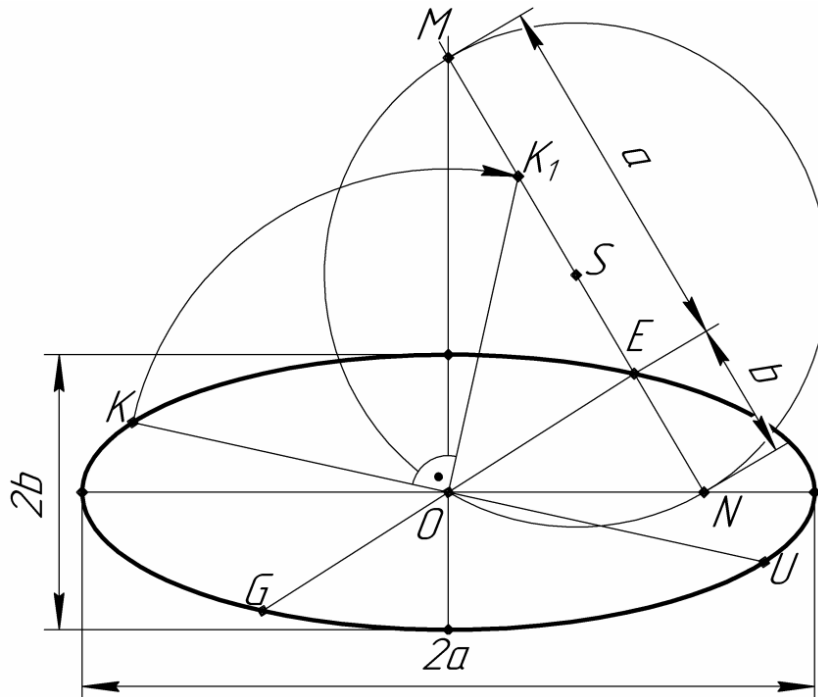


Рис. 7. Построение эллипса по заданной паре его сопряженных диаметров

Список литературы

- [1]. А.В. Бубенников, М.Я. Громов. Начертательная геометрия: Учебное пособие. – М.: Высш. школа, 1973. – 416 с.

Зуев Алексей Михайлович – старший преподаватель КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: zam@bmstu-kaluga.ru

Зайчиков Никита Евгеньевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: nekit2076@yandex.ru

СЕКЦИЯ 15.

**СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ
АСПЕКТЫ ЭКОНОМИКИ**

ПРОБЛЕМЫ ОРГАНИЗАЦИИ ПРОИЗВОДСТВА В ПЕРИОД ПАНДЕМИИ

В конце 2019 года мир столкнулся с глобальной проблемой именуемой COVID-19. Летальные исходы, быстрое распространение инфекции и отсутствие вакцины или какого-либо продуманного метода лечения заболевших привели к необходимости введения карантина и самоизоляции в начале 2020 года во многих странах мира, в том числе и в России. В России режим самоизоляции продлился несколько месяцев, но, несмотря на это, нанесенный экономике страны, малому бизнесу и отдельным производствам ущерб был весьма значительным. Экономика впервые за несколько лет столкнулась с массовым сокращением потребительского спроса в разных сферах, а также отсутствием работников на рабочих местах, что значительно сказалось на многих аспектах производства. Предприятия столкнулись с проблемой организации производства в период пандемии.

Организация производства представляет собой вид деятельности по объединению всех составляющих производственного процесса, который обеспечивает взаимодействие всех элементов производства с целью наилучшего использования производственных ресурсов и достижения поставленных задач в кратчайшие сроки.

Основной задачей организации производства является соблюдение необходимого баланса между факторами производства: организация рабочих мест, распределение трудовых заданий между работниками, согласование времени выполнения операций по цехам и т.д.

Эффективность производства напрямую зависит от условий и организации труда работников. Поэтому организация производства является обязательным условием ритмичной работы любого предприятия, так как создает благоприятные условия для высокопроизводительной работы, выпуска продукции высокого качества, полного использования всех ресурсов предприятия, в том числе и кадровые.

Кадровые ресурсы представляют собой совокупность всех сотрудников организации, обладающих определенными навыками и знаниями и объединенных для совместной трудовой деятельности. Именно это важное звено оказалась под ударом из-за ситуации с COVID-19 не только в нашей стране, но и во всем мире. В начале 2020 года возрастает число заболевших работников, что сказывается на работе предприятия: план не выполняется в сроки, снижается качество продукции и т.д.

С введением режима самоизоляции ситуация усложняется. Перед предприятием встает проблема выбора тех работников, чье присутствие на предприятии необходимо, а также в определении тех сотрудников, которые могут выполнять свою работу удаленно.

Удаленная или дистанционная работа – новая форма трудовой деятельности, широко распространившаяся в период самоизоляции. Взаимодействие сотрудников между собой и с руководителями осуществляется через Интернет, а также с помощью видеосвязи. Для видеосвязи используют такие платформы, как Skype, Zoom, Discord и др., которые также используются для проведения различного рода конференций. При передаче через интернет конфиденциальной информации, возрастает риск промышленного шпионажа, что приводит к необходимости продуманного способа защиты передаваемых данных.

При этом не каждый может с легкостью настроиться на работу в домашних условиях. Рекомендуется в начале рабочего дня производить своеобразную переключку сотрудников в групповых чатах, составить рабочий план и определить объем работы, который необходимо выполнить к концу дня.

При этом не стоит забывать о важности информационного взаимодействия между руководителями, специалистами и остальными участниками производства. Для решения этой проблемы необходимо назначить контактное лицо, которое будет отвечать за связь между разными структурными подразделениями компании. Чтобы связь между подразделениями осуществлялась с большой точностью, руководители должны убедиться в том, что сотрудники обладают необходимым оборудованием для осуществления и поддержания связи друг с другом, а также имеют доступ к необходимым данным для удаленного выполнения своих обязанностей.

Также не следует забывать об обязательных мерах безопасности на предприятии, введенных в связи с быстрым распространением инфекции, а именно обязательное ношение масок, обработка антисептическими препаратами, иными средствами и способами оборудования и производственных помещений и пр. При этом обработка оборудования и помещений занимает определенное время. Поэтому необходимо пересмотреть рабочий график и внести в него изменения так, чтобы с определенной периодичностью осуществлялись необходимые санитарные мероприятия, а их проведение не мешало производственному процессу.

Несмотря на возникшие сложности, предприятие должно продолжать взаимодействовать с клиентом и по возможности установить новые сроки производства и сбыта продукции, которые будут устраивать обе стороны. Как было сказано ранее, из-за ситуации с пандемией время на производство одного готового изделия увеличивается, следовательно, увеличивается время выполнения заказа. Транспортировка, если она требуется, также требует определенного времени. Поэтому от правильной организации действий всех подразделений предприятия зависит не только прибыль, но и имидж компании в глазах потребителей.

Организация производства в период пандемии – полезный опыт не только для руководителей предприятий, но и для отдельных его сотрудников. Ситуация с коронавирусом и самоизоляцией показала, что предприниматели не всегда могут корректно использовать свои организаторские способности и применять их в критических или неординарных ситуациях. Следовательно, пред-

приятия всегда должны рассматривать возможность непредвиденных обстоятельств, которые в той или иной степени могут повлиять на процесс производства, и по возможности сразу реагировать на них.

Необходимы инновации, которые будут действенны и при нормальных, и при непредвиденных условиях труда. Таким образом, пандемия – это лишь стимул для разработки новых способов организации производства.

Список литературы

[1]. *Энциклопедия* производственного менеджера. Организация производства. [Электронный ресурс]. – Режим доступа: <http://www.up-pro.ru/encyclopedia/organizaciya-proizvodstva.html>

[2]. *Воздействие* пандемии COVID-19 на промышленность и экологию. [Электронный ресурс]. – Режим доступа: <https://ach.gov.ru/upload/pdf/Covid-19-prom.pdf>

[3]. *COVID-19* и планирование в условиях пандемии. Какие ответные меры должны принять компании. [Электронный ресурс]. – Режим доступа: https://www.ey.com/ru_ru/covid-19/covid-19-and-pandemic-planning--how-companies-should-respond#chapter-1500816810

[4]. *Переход* на дистанционную работу в условиях коронавируса: возможные способы. [Электронный ресурс]. – Режим доступа: <http://www.garant.ru/news/1332617/>

Полякова Тамара Шериповна – студент МК8-31Б КФ МГТУ им. Н.Э. Баумана. E-mail: tamarapolakova02@gmail.com

РОЛЬ ТЕХНОЛОГИЧЕСКИХ ИННОВАЦИЙ В ЭКОНОМИКЕ ШЕСТОГО ИНДУСТРИАЛЬНОГО УКЛАДА

Для управления технологическими инновациями в современной экономике необходим анализ и вытекающие из него выводы о движущих силах и инструментах управления производительными силами и производственными отношениями в различных технологических укладах на всех этапах развития общества.

Использование концепции технологических укладов как методологической основы для анализа управленческой основы при оценке технологических инноваций позволило оценить условия вхождения экономик пятого индустриального уклада в шестой, базирующийся на его основных научных достижениях.

Рассматривая концепцию технологических укладов как инструмент оценки отечественной экономики после деиндустриализации Российской Федерации (РФ) в 90-е годы прошлого столетия, можно с большой долей вероятности констатировать, что в настоящее время в ней преобладают технологии, методы организации производства и управления, соответствующие четвертому технологическому укладу, в то время как экономически развитые страны мирового сообщества постепенно уже вступают в шестой технологический уклад, технологическим ядром которого являются нанотехнологии, нанобиотехнологии, микроэлектронные технологии, нанороботизация и другие наноразмерные производства [1].

Технологии шестого технологического уклада приведут к существенному снижению ресурсоемкости производства, его капиталоемкости, трудоемкости, материалоемкости при безусловном росте наукоемкости производства. Возможности этих технологий позволят синтезировать материалы с необходимыми свойствами, сократить размерный масштаб предметов труда, повысить на этой основе эффективность использования всех видов ресурсов [1, 2].

В условиях ограниченности финансовых ресурсов для обеспечения экономической безопасности государства требуется ускоренное технико-технологическое развитие национальной экономики, её отраслей и отдельных хозяйствующих субъектов на новой технологической платформе.

Совершенно очевидно, что для ликвидации наблюдаемого в РФ технико-технологического отставания необходима, во-первых, разработка эффективного инструментария оценки организационно-технологической, экономической и экологической эффективности технологических инноваций, степени их соответствия тенденциям мирового технологического развития, а во вторых, создание соответствующих организационных, финансовых, экономических условий, способствующих эффективному решению поставленной задачи.

Анализируя условия, в которых ранее осуществлялись переходы от одного технологического уклада к другому, можно констатировать взаимозависи-

мость, взаимообусловленность и параллельность в развитии технической базы производства и её организационно-управленческой инфраструктуры на всех уровнях управления – от государственного до отдельного хозяйствующего субъекта.

Вышеприведенное дает основание предположить, что разработка эффективного инструментария оценки организационно-технологической и экономической эффективности технологических инноваций, степени их соответствия современным тенденциям технологического развития, должна строиться с учетом анализа существующих в мировой практике подходов, включая развитие и совершенствование критериев и инструментов оценки организационно-технологической, экономической и экологической эффективности технологических инноваций [3-5].

Методологической базой такого инструментария может служить концепция организационно-технологических инноваций в различных укладах [6].

Использование концепции технологических укладов как методологической основы для создания управленческого инструментария комплексной оценки эффективности технологических инноваций, управления развитием и сменой самих технологических укладов требует совершенствования методологии измерения степени существующего технико-экономического состояния, разработки количественных и качественных параметров, характеризующих уровень развития того или иного технологического уклада, а также критериев оценки его эффективности.

Использование аппарата производственных функций, моделей межотраслевых балансов, различных подходов к определению эффекта научно-технического прогресса, как измерителей уровня технико-технологического развития и эффективности технологического уклада, возможно только на макроуровне и реализуемо на микроуровне, например, для отдельных акционерных обществ (АО) и других хозяйствующих субъектов (экономически минимальных производственных систем). Их анализ позволяет утверждать, что концепция технологических укладов прикладного экономического инструментария дает возможность оценивать комплексную эффективность технологических проектов (организационно-техническую, экономическую, финансовую, экологическую), реализуемых в рамках отдельных хозяйствующих субъектов, а также и их соответствие тому или иному технологическому укладу. При этом необходимо оценивать не только чисто технические аспекты проектов, но и связанные с ними организационно-экономические, информационно-прикладные, кадровые, интеллектуальные особенности производства. Указанное обстоятельство определяет актуальность разработки эффективной управленческой системы.

Глобальное управление развитием и сменой будущих технологических укладов должно базироваться на основе исследований и анализа особенностей уже прошедших укладов. Оно требует и создания соответствующего организационно-экономического механизма регулирования такого управления, направленного на выработку комплекса всех необходимых условий как макро-

экономического, так и микроэкономического характера. В первую очередь речь идет о разработке эффективной системы управления, учитывающей особенности и целевое назначение каждой фазы жизненного цикла технологического уклада, поскольку он – это не только система сопряженных отраслей и производств, характеризующихся единой технико-технологической базой, но и, главное, это определенный тип производственных отношений с особой системой хозяйственной, организационной и управленческой деятельности аспектов уклада [6].

При этом необходимо отметить, что технологическая революция, реализованная в пятом технологическом укладе, привела к цифровизации экономики, к формированию системы производственных отношений, основанных на использовании цифровых информационно-коммуникационных технологий. Цифровая экономика – это система производственных отношений, реализуемых через такие платформы, как Интернет, а также мобильные и сенсорные сети. По сути, это модель экономики, основанной на возможностях, которые предоставляет доступ в Интернет.

При становлении цифровой экономики использованы три элемента – инфраструктура (доступ в Интернет, программное обеспечение, телекоммуникации), электронный бизнес (ведение хозяйственной деятельности через компьютерные сети), электронная коммерция (электронная продажа продукции, работ, услуг).

В условиях цифровой экономики большинство бизнес-процессов, особенно в сфере управления предприятиями, осуществлялось в онлайн-режимах (заключение и сопровождение договоров, реализация продукции, работ, услуг, логистические операции, финансово-бухгалтерские операции, подготовка и переподготовка кадров, электронный документооборот и т.п.). Современные цифровые технологии существенно снизили себестоимость, улучшили качество продукции, уменьшили процент брака и повысили производительность труда, способствуя росту конкурентоспособности АО, что и мотивировало их практическое применение. В этих условиях существенно возрос уровень автоматизации производства, повысилась его гибкость и мобильность [7].

Стоимость бизнеса, как комплексный показатель эффективности его развития, стала основным показателем, по которому оценивают и ранжируют технологические и другие инновации, особенно относящиеся к классу инвестиционно-емких инноваций [8].

Оказалось, что рыночная стоимость бизнеса АО отражает целевые устремления собственников бизнеса и его инвесторов, так как они преследуют цель увеличения получаемых доходов, достижение которой возможно только при условии роста стоимости бизнеса. Это связано с присущим стоимостной концепции несовершенством методологии измерения технико-экономического развития, отсутствием количественных и качественных параметров, характеризующих уровень развития того или иного технологического уклада.

Критерием оценки эффективности технологических инноваций в 5-ом цикле являлась рыночная стоимость бизнеса.

Шестой технологический уклад в соответствии с [6] реализуется в период 2020-2050-е годы, а все его составляющие носят характер прогноза. В нем дальнейшее развитие получают робототехника, биотехнологии, основанные на молекулярной и геномной инженерии, космические технологии, а также интеллектуальная продукция.

Ключевой фактор в нем – молекулярные, клеточные и ядерные технологии, управление поведением атомных и молекулярных объектов.

Технологии, созданные в шестом технологическом укладе, приведут к существенному снижению ресурсоемкости производства, его капиталоемкости, трудоемкости, материалоемкости и, при безусловном росте, наукоемкости, которые будут основаны на новых композиционных материалах и возобновляемых источниках энергии.

Текущие затраты, связанные с технологической инновацией, в таком случае необходимо рассчитывать исходя из условий о том, что производственный (технологический и трудовой) процесс осуществляется в полном соответствии с технологическим регламентом: производственные мощности АО полностью загружены, соблюдаются установленные нормы расходов ресурсов, соответствующие использованию системы стандарт-кост, как системы учета и управления затратами, отсутствуют непредвиденные простои оборудования. Можно резюмировать: предельно эффективная технология может использоваться как расчетная модель оценки организационно-технической и экономической эффективности инноваций при соблюдении экологических требований к производственному процессу. Она позволяет рассчитать ожидаемые технико-экономические показатели любой гипотетической технологии при относительно малой погрешности.

Исходя из оценки входа различных экономик в 6-ой технологический уклад и проанализировав технологические и трудовые процессы, реализуемые в экономике РФ, можно констатировать, что в последнюю четверть века негативные последствия деиндустриализации не позволили восстановить в ней необходимую сеть обрабатывающих производств, хотя есть определенные достижения в оборонно-промышленном комплексе, сельском хозяйстве и торговле. Поступательное вхождение в 6-ой технологический уклад будет базироваться на позитивном влиянии вышеприведенных отраслей на другие виды экономики.

Основными движущими силами в соответствии с предложенными выше критериями будут национальные проекты [9] и реализуемые в рамках национального проекта «Наука», и приходящему ему на смену нацпроекту «Наука и университеты», научно-образовательные центры (НОЦ). Поскольку в НОЦ будут аккумулированы бюджетные и внебюджетные финансовые средства, то научно-образовательный потенциал РФ будет активно влиять на экономику 6-го технологического уклада не только из НОЦ мирового уровня, но и из других центров [10] и АО.

Несмотря на естественные потери в экономике РФ в условиях мирового кризиса, разразившегося в связи с распространением новой коронавирусной

инфекции COVID-19, повсеместно снизившие темпы роста экономик, это не повлияет на основные показатели реально достижимых технологий 6-го технологического уклада.

Список литературы

- [1]. *Марин В.П., Федоров В.К., Луценко А.В.* Основы теории нанотехнологий: Монография. – М.: Изд-во МАТИ, 2013. – 128 с.
- [2]. Молекулярная биотехнология. Принципы и применение: пер. с англ. / Б. Глинк, Дж. Пастернак. – М.: Мир, 2002. – 589 с.
- [3]. *Кун Т.С.* Структура научных революций. – М.: Наука, 1975. – 115 с.
- [4]. *Суханов А.Д., Голубева О.Н.* Концепция современного естествознания. – М.: Дорфа, 2004. – 256 с.
- [5]. *Богданкевич О.В.* Лекции по экологии. – М.: Физматлит, 2002. – 208 с.
- [6]. *Тебекин А.В., Серяков Г.Н.* Влияние динамики циклов экономической активности на перспективы развития национальной экономики // Проблемы современной экономики. – 2015. – № 1. – С. 34-38.
- [7]. Нанотехнологии как ключевой фактор нового технологического уклада в экономике / Под ред. *С.Ю. Глазьева и В.В. Харитонова.* – М.: Тривант, 2009. – 304 с.
- [8]. *Лаврухина Н.В., Перерва О.Л.* Стоимостная концепция и оценочные технологии управления инновационными предприятиями: Учебное пособие. – М.: МГТУ им. Н.Э. Баумана, 2013. – 243 с.
- [9]. Национальные проекты: будущее России [Электронный ресурс] // <https://futuregerussia.gov.ru/> (Дата обращения 20.10.2020).
- [10]. *Марин В.П., Челенко А.В., Шмаков Н.В., Коржавый А.П.* Эффективность научно-образовательных центров, функционирующих в промышленно-развитых муниципальных образованиях // Научно-технологические технологии. – 2019. – Т. 20, № 2. – С. 66-73.

Челенко Александра Викторовна – доцент кафедры, канд. техн. наук
КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail:
apererva@yandex.ru

СУЩНОСТЬ ПОЛИТИКИ КОНКУРЕНТОСПОСОБНОСТИ, ОСОБЕННОСТИ ФОРМИРОВАНИЯ И МЕХАНИЗМЫ ЕЁ РЕАЛИЗАЦИИ

Конкурентоспособность определяется по отношению либо к конкретному рынку, либо к конкретной группе потребителей, в соответствии определённой сегментацией рынка. Если конкурентоспособный объект не указан на каком-либо рынке, это значит, что объект в данный момент является лучшим мировым образцом и не имеет аналогов. Создание конкурентных приоритетов и их поддержание позволяет обеспечивать конкурентоспособность на рынке [3, С. 42].

Конкуренция со стороны возможных конкурентов может возникнуть тогда, когда есть вероятность, что организации других отраслей могут начать реализовывать продукцию других отраслей. Угроза со стороны других конкурентов соответствует величине барьера входа в отрасль и спецификой отношений в данной отрасли. Величин входного барьера могут определять следующие факторы:

1. Производственный и маркетинговый эффекты масштаба освоения.
2. Наличие каналов сбыта.
3. Жесткость государственного регулирования [4, С. 66].

Количество отраслевых организаций связано с уровнем конкуренции и темпом развития рынка, таким образом, чем выше количество организаций, тем выше конкуренция, и, чем выше интенсивность конкуренции, тем медленнее развивается рынок. При вхождении сильных компаний на рынок, интенсивность конкуренции, как правило, увеличивается, это связано с желанием таких фирм достигнуть лидирующих позиций, что вполне аргументировано, так как их позиции подкреплены мощным финансовым положением.

Существует много способов конкуренции и стратегий предприятия: производственная, товарная, ценовая и прочая. В основе любой стратегии находятся конкурентные преимущества. Иными словами стратегическое управление есть управление конкурентными преимуществами. Конкурентное преимущество – это способность предприятия и его состояние на рынке, которые участвуют в преодолении конкуренции и участвуют в привлечении потребителей. Конкурентные преимущества являются важной составляющей стратегии предприятия.

Наиболее общими направлениями в приобретении конкурентных преимуществ являются:

1. Лидерство в себестоимости продукции.
2. Дифференциация продукции.
3. Концентрация.
4. Стратегия первопроходца (наиболее ранний выход на рынок).
5. Известная торговая марка.

6. Гибкость в использовании ресурсов.
7. Связи с важными покупателями.
8. Наибольшая доля рынка с учетом экономии на размерах производства.
9. Возможность уменьшения затрат.
10. Использование прогрессивных технологических процессов, увеличение числа высококвалифицированных специалистов [2, С.41].

Основой поддержания конкурентной борьбы выступает процесс удержания, развития и создания преимуществ в конкуренции. Большое количество попыток понять конкурентные способности страны были разрушены из-за неверного понимания причины того, как фирма в такой стране может создать и удерживать конкурентную борьбу в отдельно взятой отрасли, и неверного подхода при создании политики в отдельной взятой фирме, без учета национальной экономики и её задачу.

При оценке конкурентоспособности рассматриваются производственные, сбытовые, рыночные возможности предприятия. Основные факторы и критерии конкурентоспособности предприятия определены в табл. 1:

Таблица 1.

Факторы и критерии конкурентоспособности предприятия

Фактор	Критерий
Производственный: 1. Имидж предприятия 2. Сертифицированная система качества 3. Применение защитных мер от фальсификации	Имидж товара
Сбытовой: 1. Количество посредников	Уровень качества: 1. Стабильность уровня
Сервисный: 1. Продолжительность гарантийного срока	Подлинность товара Потребительская новизна
Рыночный: 1. Рыночная новизна	Цена потребления товара: 1. Цена товара 2. Текущие затраты

Среди факторов определяющих конкурентоспособность фирмы можно также выделить способность создания новейших продуктов, способность в кратчайшие сроки освоения новейших продуктов и их серийного создания, уменьшение издержек на создание продукции, возможность послепродажного обслуживания. Для определения причин в осуществлении конкурентоспособности страны, необходимо более точно изучать роль в конкурентной борьбе в отрасли. Выделяют следующие виды конкурентных преимуществ:

1. Ресурсные – обуславливаются доступность природных ресурсов и рабочей силы, связаны с налоговыми режимами, выгодным местоположением и доступом к недвижимости;

2. Технологические – связаны с использованием технологий массового производства, которые обеспечивают экономию в масштабном производстве, связаны с производством продукции старой номенклатуры;

3. Инновационные – основаны на реализации НИОКР, обеспечивают обновление номенклатуры и увеличение ассортимента продукции;

4. Глобальные – обуславливаются созданием экологических и социальных стандартов, которые используются в политике государства и организаций;

5. Культурные – связаны с культурной схожестью, фирмы могут иметь рынки сбыта в странах с близкой культурой [1, С.64].

Таким образом конкурентоспособность является главным фактором успеха предприятия, поэтому должно обеспечиваться сочетание качества, цены и последующего обслуживания продукции. Конкурентные преимущества могут реализовываться в разных направлениях. Конкурентное преимущество является важным критерием в обеспечении эффективной деятельности предприятия и привлечении клиентов.

Список литературы

[1]. *Васильев В.А.* Управление качеством, подготовка кадров и организация конкурентоспособного высокотехнологичного производства / В.А. Васильев, С.В. Александрова // Научные исследования в машиностроении. – 2018. – № 4. – С. 38-43. – [Электронный ресурс] Режим доступа: <https://e.lanbook.com/journal/issue/312209>. (дата обращения: 28.04.2020).

[2]. *Комянчина К.В.* Управление качеством как новая функция и черта современного менеджмента / К.В. Комянчина // Вестник Южно-Уральского государственного университета. Серия: Социально-гуманитарные науки. – 2016. – № 3. – С. 68-72. – [Электронный ресурс] Режим доступа: <https://e.lanbook.com/journal/issue/308403>. (дата обращения: 28.04.2020).

[3]. *Леонов О.А.* Управление качеством: учебник / О.А. Леонов, Г.Н. Темасова, Ю.Г. Вергазова. – СПб.: Лань, 2020. – 180 с. – Режим доступа: <https://e.lanbook.com/book/130492>. (дата обращения: 20.02.2020).

[4]. *Майоров А.А.* Организационно-экономические аспекты управления качеством инновационной деятельности / А.А. Майоров // Интеллект. Инновации. Инвестиции. – 2015. – № 1. – С. 63-68. – [Электронный ресурс] Режим доступа: <https://e.lanbook.com/journal/issue/300518>. – (дата обращения: 28.04.2020).

Иванов Станислав Юрьевич – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: stas.ivanov20@gmail.com

Неклюдова Ирина Витальевна – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: niv150320@gmail.com

Квашина Вера Владимировна – старший преподаватель КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: vek74@inbox.ru

ЭКОНОМИКА РОССИИ ВО ВРЕМЯ ПАНДЕМИИ КОРОНАВИРУСА И МЕТОДЫ ПОДДЕРЖКИ БИЗНЕСА

Что же такое COVID-19? COVID-19 – это инфекционное заболевание, вызываемое коронавирусом SARS-CoV-2, который является респираторным патогеном.

Многие ведущие российские экономисты говорят о тревожном положении в стране. По их мнениям, из-за пандемии коронавируса и её последствий ВВП России может упасть. В 2020 году ВВП снизится на 5%, специалисты подразумевают что к 021 году ВВП составит 2,8%, об этом в своем сообщении рассказал Минэкономразвития.

Руководитель экономической экспертной группы (ЭЭГ) Евсей Гурвич в своем выступлении сказал, что в России уготовано пять шоков [4, С. 2].

Специфика России, по его мнению, заключается в том, что для нее мировой кризис (первый шок) пришел вместе с падением цен на нефть (второй шок): как сообщает профессор Высшей школы экономики Олег Вьюгин: «Падение спроса на нефть составило около 30%». Третий шок-отток капитала: «Во время любого кризиса наблюдается бегство капитала в самые развитые экономики». «Мир уже никогда не будет прежним, изменится и экономика, и её структура. В прежнем объеме спроса на нефть больше не будет, а механизмы по сокращению будут давать только краткосрочный эффект», – сообщает Николаев. Четвертый шок-это изоляция, в результате которой будет ограничение передвижения товаров и людей. Пятым шоком стала высочайшая степень неопределенности, из-за которой бизнес лишается возможности строить планы на будущее. Наиболее восприимчивым в России стал сектор услуг, микро и малый бизнес, самозанятые и большие города, где велика доля сервисной экономики. Сообщает директор Института анализа предприятий и рынков НИУ и ВШЭ Андрей Яковлев [4, С. 2].

По мнению Росстата ВВП по итогам 2 квартала 2020 года уменьшился на 8,5% по сравнению с периодом прошлого года [1, С. 2].

Ведомства сообщают, что единственным сектором, который показал рост, оказалось сельское хозяйство, выросшее на 3,1%.

Самое крупное падение было выявлено в сырьевом секторе (снизилось на 8,5%), розничной торговле (сократилась на 16,6%), пассажирских перевозках (снизились на 79,0%), а также в отраслях, которые связаны с оказанием услуг населению (сократилось на 48,9%). Меньше всего падение было замечено в обрабатывающих производствах, строительстве, оптовой торговле и грузоперевозках, а также в обеспечении электрической энергией, газом и паром и кондиционировании воздуха как сообщает Росстат.

Некоторые российские экономисты предлагают решения:

Андрей Яковлев сообщает в своем высказывании, что сегодня нет достаточного набора инструментов для поддержки малого бизнеса и самозанятых [5, С. 2].

Он предлагает создать специальную программу поддержки сектора по аналогии с ФРГ, которой должны управлять региональные власти, а средства на нее выделит федеральный центр [5, С. 2]. Объем средств и реестр потенциальных получателей помощи возможно составить на основе данных Федеральной налоговой службы. Собирать заявления и проводить выплаты можно через госбанки.

Рубен Ениколопов соглашается с тем, что малый бизнес, который не имеет подушки ликвидности, и люди, которые потеряли работу, являются наиболее пострадавшими категориями. Кроме того, необходима поддержка ключевых звеньев в производственных цепочках – если они разорятся, то выйти из кризиса будет гораздо сложнее [5, С. 2].

Проректор Всероссийской академии внешней торговли Наталья Волчкова утверждает, что основной объем помощи должен идти не через субсидии предприятиям, а через пособие по безработице [5, С. 2].

Юрий Симачев, профессор, директор по экономической политике НИУ ВШЭ, соглашается с тем, что надо субсидировать зарплаты в секторе малого и среднего бизнеса [5, С. 2].

В Росси применился проект механизма отсрочки по выплате кредитных платежей для малого и среднего бизнеса, которые пострадали во время пандемии коронавируса. Оплату процентных платежей за полгода планируется разделить поровну между государством, банками и самими предпринимателями, рассказал РБК один из представителей бизнеса, участвовавший в обсуждении вопроса с Минэкономразвития и банковским сектором. По моему мнению для России будет выгодней всего использовать метод Андрея Яковлева который заключается в том, что поддержкой сектора должны управлять региональные власти, а средства на нее выделит федеральный центр и как высказывается Симачев, надо субсидировать зарплаты в малом и среднем бизнесе.

В Минэкономразвития предполагают, что активная фаза восстановления экономики России начнется в 4 квартале текущего года и продолжится в 2021 году.[3, С. 23]

Список литературы

- [1]. [bbc.com/russian/news-53741291](https://www.bbc.com/russian/news-53741291)
- [2]. https://1prime.ru/state_regulation/20200522/831492612.html
- [3]. <https://rg.ru/2020/07/07/finansist-obiasnil-ustojchivost-ekonomiki-rossii-vo-vremia-pandemii.html>
- [4]. <https://www.dw.com/ru>
- [5]. <https://www.hse.ru/news/expertise/358154684.html>
- [6]. <https://www.rbc.ru/rbcfreenews/5f9d5a6e9a7947fec3b3270b>

Кузнецова Анастасия Дмитриевна – студент МК8-32Б. E-mail: nastakuz2001@mail.ru

СЕКЦИЯ 16.

**ОБЩЕСТВЕННО-ПОЛИТИЧЕСКИЕ
И ФИЛОСОФСКИЕ ВОПРОСЫ
РАЗВИТИЯ ОБЩЕСТВА**

КАРАБАХ СНОВА В ОГНЕ: ПОЧЕМУ СЕГОДНЯ?!

Армения и Азербайджан в настоящее время на грани большой войны из-за Карабаха. Танки, авиация, артиллерия – все военные средства задействованы в зоне конфликта, обстреливаются населенные пункты, а главное – гибнут люди.

Конфликт в Нагорном Карабахе казался давно замороженным, почему вдруг резко включился процесс разморозки? Чтобы ответить на этот вопрос, обратимся к началу его истории.

Армянские исторические источники утверждают, что Арцах (древнеармянское название) впервые упоминается еще в VIII веке до н.э. Если верить этим источникам, то Нагорный Карабах являлся частью Армении еще в период раннего Средневековья. В результате завоевательных войн Турции и Ирана в эту эпоху значительная часть Армении перешла под контроль данных стран. Армянские княжества, или меликства, на тот момент располагавшиеся на территории современного Карабаха, сохранили полунезависимый статус.

Свою точку зрения в этом вопросе представляет Азербайджан. По мнению местных исследователей, Карабах является одним из самых древних исторических регионов их страны. Слово «карабах» по-азербайджански переводится как «гара», что означает черный, и «баг» – сад. Уже в XVI веке вместе с другими провинциями Карабах находился в составе государства Сефевидов, а после стал независимым ханством.

В 1805 году Карабахское ханство было подчинено Российской Империи, а в 1813 по Гюлистанскому мирному договору в состав России вошел и Нагорный Карабах. Затем, по Туркменчайскому договору, а также соглашению, заключенному в городе Эдирне, производилось переселение армян из Турции и Ирана и размещение их на территориях Северного Азербайджана, в том числе и в Карабахе. Таким образом, население этих земель имеет преимущественно армянское происхождение.

В 1918 году контроль над Карабахом получила только что созданная Азербайджанская Демократическая Республика. Практически одновременно на эту местность выдвигает претензии Армянская Республика, но АДР данные притязания не признает. В 1921 году территория Нагорного Карабаха с правами широкой автономии включается в состав Азербайджанской ССР. Еще через два года Карабах получает статус автономной области (НКАО). В 1988 году Совет депутатов НКАО ходатайствует к властям АзССР и АрмССР республик и предлагает передать спорную территорию в состав Армении. Это ходатайство не было удовлетворено, вследствие чего по городам Нагорно-Карабахской АО прокатилась волна протеста. Демонстрации солидарности проводились также и в Ереване.

В начале осени 1991 года, когда Советский Союз уже начал разваливаться, в НКАО принимается Декларация, провозгласившая Нагорно-Карабахскую

Республику. Причем помимо НКАО, в её состав вошла часть территорий бывшей АзССР. По результатам референдума, проведенного 10 декабря того же года в Нагорном Карабахе, более 99% населения региона проголосовало за полную независимость от Азербайджана.

Вполне очевидно, что властями Азербайджана данный референдум признан не был, а сам акт провозглашения обозначили как незаконный. Более того, в Баку приняли решение упразднить автономию Карабаха, которой он обладал в советское время. Однако разрушительный процесс уже был запущен. За независимость самопровозглашенной республики встали армянские отряды, которым попытался противостоять Азербайджан. Нагорный Карабах получил поддержку от официального Еревана, а также от национальной диаспоры в других странах, поэтому ополчению удалось отстоять регион. Впрочем, властям Азербайджана все-таки удалось установить контроль над несколькими районами, которые изначально были провозглашены частью НКР.

Переговоры, в ходе которых стороны пытались урегулировать конфликт мирным путем, начались практически сразу после того как была провозглашена независимая НКР. Например, 23 сентября 1991 года состоялась встреча, на которой присутствовали президенты Азербайджана, Армении, а также России и Казахстана.

Весной 1992 года ОБСЕ была учреждена группа по урегулированию карабахского конфликта. Несмотря на все попытки международного сообщества остановить кровопролитие, прекратить огонь удалось лишь весной 1994 года. 5 мая в столице Киргизии был подписан Бишкекский протокол, после чего участники прекратили огонь уже спустя неделю.

Стороны конфликта так и не сумели договориться по поводу итогового статуса Нагорного Карабаха. Азербайджан требует уважать его суверенитет и настаивает на сохранении территориальной целостности. Интересы самопровозглашенной республики защищает Армения. Нагорный Карабах выступает за мирное разрешение спорных моментов, при этом власти республики подчеркивают, что НКР способна постоять за свою независимость. Но окончание военных действий не означало, что наступил мир. Это была лишь временная заморозка конфликта.

Таким образом, одна из причин происходящего – это отсутствие политического урегулирования конфликта компромиссом, с которым бы согласились обе стороны. Болезнь подлечена, но не вылечена.

Не секрет и то, что это очередная попытка проверки на политическую прочность России, т.к. Армения член ОДКБ, и если будет нарушена территория Армении, то член ОДКБ обязан вмешаться в конфликт. Азербайджан также давний партнер России, и эти обострения отношений РФ совершенно не нужны.

По мнению политолога Михеева С.А. во всей ситуации разогрева конфликта немаловажную роль играет Турция. В её интересах влияние на Азербайджан, поэтому, скорее всего Турция в лице Р. Эрдогана будет «подливать масла в огонь». Что касается западных стран и США, они ведут двойную игру:

1) столкнуть Россию и Турцию;

2) в случае если Армения обратится за помощью к США, можно взять её под патронаж, учитывая, что в настоящее время там прозападное руководство.

Кроме того, есть причина внутреннего политического плана в самом Азербайджане. Клан Алиева давно у власти, и в его интересах продлить легитимность азербайджанской политической модели за счет решения карабахского вопроса. Также как и Н. Пашиняну, чтобы удержаться у власти, нужна победа. Наконец, конфликт, вспыхнувший именно сейчас – это мировой экономический кризис на фоне пандемии коронавируса. Война ведь многое может списать. Но это для политиков, а вот для тех, кто гибнет под обстрелами с обеих сторон, нужен мир. Российская сторона по средствам дипломатических переговоров на разных уровнях прилагает все усилия для прекращения конфликта. Хотелось бы, чтобы здравый разум восторжествовал над амбициями политиков, было найдено мирное решение вопроса в долгую.

Список литературы

[1]. *Внезапная «разморозка» конфликтов*: политолог Сергей Михеев о волнениях в бывших союзных республиках. [видеозапись] – URL: <https://russian.rt.com/ussr/video/788583-politolog-intervyu-nagorny-karabah-belorussia>.

[2]. *Нагорный Карабах. История и суть конфликта*. [Электронный ресурс] – URL: <https://fb.ru/article/207937/nagornyiy-karabah-istoriya-i-sut-konflikta>.

Азаренко Инна Сергеевна – старший преподаватель, канд. техн. наук
КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail:
89108651131@mail.ru

Егоренкова Юлия Вадимовна – студент. E-mail: ulia.eg@yandex.ru

И.Д. Стадникова, Т.В. Шафигуллина

ОБЩЕСТВЕННЫЙ КОНТРОЛЬ: ЗАКОНОДАТЕЛЬНОЕ ЗАКРЕПЛЕНИЕ

Основная задача любого демократического государства – обеспечение конституционных прав и свобод человека и гражданина. Эффективность деятельности власти определяется как качеством выполняемых ею обязанностей, так и устойчивостью её обратной связи с обществом.

Общественный контроль – это механизм, который позволяет обществу контролировать власть, как на этапе принятия, так и на этапе реализации решений и оценки полученного результата.

Современные тенденции развития общественно-политической системы страны, активизация гражданского общества, возросшие требования к повышению эффективности функционирования системы государственного управления повысили социальный запрос на масштабы и качество общественного контроля в нашей стране.

В этих условиях существенно возросло значение системы общественного контроля и его различных звеньев, что позволяет избежать нарастания социального недовольства и противостояния гражданского общества и государственной власти.

Общественный контроль является одной из форм гражданского участия, имеющего большую значимость для стабильного развития демократического общества. Контроль со стороны общества за деятельностью органов власти служит основой демократического политического устройства [1, 71].

Обязательность существования института общественного контроля в демократическом обществе – общепризнанный принцип международного права. Специальный докладчик Комиссии по правам человека ООН г-жа К.К. Куфа отметила, что демократическое общество независимо от его культурной, политической, социальной и экономической основы определяется такими принципами и институтами как плюрализм, верховенство права, законность, политическое равноправие, общественный контроль и подотчетность правительства обществу [1, 35].

Формирование гражданского общества и построение правового государства в России актуализируют вопросы осуществления общественного контроля во всех сферах государственной жизни.

Г.В.Ф. Гегель писал: «Обеспечение государства и тех кто находится под его управлением от злоупотреблений властью ведомствами и их чиновниками заключается, с одной стороны, непосредственно в их иерархии и ответственности, с другой – в правах общин, корпораций, посредством чего привнесению субъективного произвола в доверенную чиновникам власть ставится для себя препятствие, и недостаточный в отдельных случаях контроль сверху дополняется контролем снизу» [2, 247].

Известно, что в правовом государстве власть должна быть подчинена праву, что достигается только путем контроля над ней. Как справедливо отмечает А.С. Панарин: «Нет ничего опаснее бесконтрольной власти, опирающейся не на закон, а на угрозу применения насилия; необходим надежный демократический контроль» [3, 11]. В свою очередь В.О. Лучин и Н.А. Боброва конкретизируют: «Способность общества к контролю над властью – признак гражданского общества. Только контроль, приобретая правовые формы, способен подчинить власть праву, и только при условии существования гражданского общества государство оказывается «под правом», становится правовым» [4, 27].

Законодательную форму общественный контроль обрел в 2014 г. с принятием закона «Об основах общественного контроля в Российской Федерации», в котором установлены правовые основы организации и осуществления общественного контроля, определяется сфера деятельности общественного контроля как правового института в Российской Федерации [5]. Впервые в российском законодательстве дается определение общественного контроля, содержится указание на цели общественного контроля, осуществляемого субъектами общественного контроля, а также указываются его сферы деятельности (ст. 4): «Деятельность субъектов общественного контроля, осуществляемая в целях наблюдения за деятельностью органов государственной власти, органов местного самоуправления, государственных и муниципальных организаций, иных органов и организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, а также в целях общественной проверки, анализа и общественной оценки издаваемых ими актов и принимаемых решений».

Ранее нормативная база общественного контроля имела фрагментарный характер. Например, Комитет РФ по земельным ресурсам и землеустройству в своем письме от 26 января 1995 г. № 3-14/166 в целях усиления общественного контроля по использованию и охране земель и привлечению широкой общественности к решению вопросов сохранения благоприятной окружающей среды утвердил «Памятку». Данный документ, регулируя деятельность внештатных общественных инспекторов по осуществлению контроля использования и охраны земель, определял цели общественного контроля, порядок назначения общественных контролеров, а также их права. В сфере труда также принимались некоторые шаги по законодательному закреплению общественного контроля. Так, гл. 58 Трудового кодекса РФ регулировала защиту трудовых прав работников профессиональными союзами. Можно назвать и Указ Президента РФ от 23 июля 2003 г. № 827, в соответствии с которым образован Общественный совет по инвестированию средств пенсионных накоплений, созданный для обеспечения общественного контроля по формированию и инвестированию средств пенсионных накоплений [6].

В современных условиях никто не станет отрицать значимость и необходимость общественного контроля, в том числе и за действиями властных структур и их чиновниками, о которых так нелицеприятно отзывался Прези-

дент Российской Федерации: «Наше чиновничество еще в значительной степени представляет собой замкнутую и подчас просто надменную касту, понимающую государственную службу как разновидность бизнеса» [7]. Поэтому так важен принятый Федеральный закон № 212, который определяет цели общественного контроля (ч. 1 ст. 5), а именно:

1) обеспечение реализации и защиты прав и свобод человека и гражданина, прав и законных интересов общественных объединений и иных негосударственных некоммерческих организаций;

2) обеспечение учета общественного мнения, предложений и рекомендаций граждан, общественных объединений и иных негосударственных некоммерческих организаций при принятии решений органами государственной власти, органами местного самоуправления, государственными и муниципальными организациями, иными органами и организациями, осуществляющими в соответствии с федеральными законами отдельные публичные полномочия;

3) общественная оценка деятельности органов публичной власти для защиты прав человека и гражданина, прав и законных интересов общественных объединений и иных негосударственных некоммерческих организаций [5].

Задачи общественного контроля, содержащиеся в ч. 1 ст.5, можно условно классифицировать, выделив в них две группы: внутренние задачи и внешние задачи. К внутренним задачам относятся задачи, непосредственно связанные с реализацией институтами общественного контроля мер, обеспечивающих общественный контроль как таковой. К ним относится, например, задача реализации гражданских инициатив, направленных на защиту прав и свобод человека и гражданина, прав и законных интересов общественных объединений и иных негосударственных некоммерческих организаций, содействие предупреждению и разрешению социальных конфликтов. К внешним задачам можно отнести задачу формирования в обществе нетерпимости к коррупционному поведению; повышения эффективности деятельности органов государственной власти, органов местного самоуправления, государственных и муниципальных организаций, иных органов и организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия; повышение уровня доверия граждан к деятельности государства, а также обеспечение тесного взаимодействия государства с институтами гражданского общества. Внутренние и внешние задачи диалектически связаны между собой. Их реализация на практике должна обеспечить достижение целей, установленных в ч. 1 ст. 5.

Закон устанавливает основополагающие принципы (ст.6) осуществления общественного контроля: приоритет прав и законных интересов человека и гражданина; добровольность участия в осуществлении общественного контроля; самостоятельность и независимость субъектов; публичность и открытость; законность; объективность, беспристрастность и добросовестность субъектов; обязательность рассмотрения органами публичной власти результатов общественного контроля; многообразие форм общественного контроля; недопустимость необоснованного вмешательства субъектов общественного

контроля в деятельность органов публичной власти и в сферу деятельности политических партий; презумпция добросовестности деятельности органов публичной власти; соблюдение нейтральности субъектами общественного контроля, исключающей возможность влияния решений политических партий на осуществление общественного контроля.

Принципы общественного контроля, содержащиеся в комментируемой статье, представляется целесообразным разделить на две группы принципов: принципы организации и деятельности общественного контроля и принципы взаимодействия субъектов и участников общественного контроля с органами государственной власти, органами местного самоуправления, государственными и муниципальными организациями, иными органами и организациями, осуществляющими в соответствии с федеральными законами отдельные публичные полномочия [1].

Указанные принципы приобретают исключительное значение в условиях формирования и развития гражданского общества и правового государства. Их закрепление позволяет определить своеобразные границы осуществления общественного контроля, одновременно устанавливая его широкую зону распространения [8].

Формы и порядок проведения общественного контроля указаны в гл 3 (ст. 18-26). Перечень форм общественного контроля включает: мониторинг, проверка, независимые экспертизы, обсуждения, публичные слушания.

Эффективность указанных форм деятельности невелика, т.к. не установлены показатели её оценки, необходима разработка соответствующего «измерителя». Одним из таких показателей может стать степень удовлетворенности населения.

Объектами общественного контроля являются: деятельность в области обеспечения обороны страны и безопасности государства, общественной безопасности и правопорядка, деятельность полиции, органов следствия, прокуратуры и судов, а также деятельность, связанная с исполнением наказаний, контролем за оборотом наркотических средств и психотропных веществ, содержанием детей-сирот и детей, оставшихся без попечения родителей, оказанием психиатрической помощи. Однако действие Федерального закона не распространяется на общественные отношения, регулируемые законодательством о выборах и референдумах. Не являются объектами общественного контроля сведения, которые представляют государственную тайну, а также сфера частной жизни граждан.

Согласно федеральному законодательству, право граждан на участие в системе общественного контроля может осуществляться как лично, так и в составе общественных объединений и иных негосударственных некоммерческих организаций. Отмечается, что граждане участвуют в осуществлении общественного контроля добровольно, и никто не вправе оказывать какое-либо воздействие на гражданина в целях принудить его к участию либо неучастию в осуществлении общественного контроля либо препятствовать реализации его права на участие в его осуществлении. Также законом установлено, что граж-

дане реализуют данное право, выступая в качестве общественных инспекторов и общественных экспертов. Помимо этого, Закон закрепляет правовое положение субъектов общественного контроля, их основные права и обязанности, способы осуществления ими общественного контроля, способы определения и обнародования результатов общественного контроля [5].

Субъектами общественного контроля, согласно статье 9 Федерального закона «Об основах общественного контроля в Российской Федерации» являются:

- 1) Общественная палата Российской Федерации;
- 2) общественные палаты субъектов Российской Федерации;
- 3) общественные палаты (советы) муниципальных образований;
- 4) общественные советы при федеральных органах исполнительной власти, общественные советы при законодательных (представительных) и исполнительных органах государственной власти субъектов Российской Федерации [5].

Помимо этого, Федеральным законом № 212-ФЗ утвержден перечень так называемых специальных субъектов общественного контроля, обеспечивающих реализацию отдельных форм общественного контроля, а именно:

- 1) общественные наблюдательные комиссии;
- 2) общественные инспекции;
- 3) группы общественного контроля;
- 4) иные организационные структуры общественного контроля.

Субъекты общественного контроля, как правило, возникают самостоятельно, по инициативе граждан, хотя сегодня отмечается преобладание субъектов, формируемых по принципу «сверху», - общественные палаты, советы и комиссии. Для них государство создает особые условия, одновременно ограничивая независимых субъектов. Однако необходимо помнить, что создание институтов гражданского общества «сверху» часто ведет к их формализации и к профанации сути общественной деятельности.

Объект общественного контроля включает все группы общественных отношений, за исключением тех, которые «закрываются» государством (объекты, сведения о которых представляют государственную тайну, а также сфера частной жизни граждан). Наибольший интерес для общественного контроля представляют, конечно же, отношения в сфере государственного управления, трудовые отношения и отношения в сфере защиты прав потребителей.

В ст. 27 не устанавливаются специальные нормы об ответственности за нарушение законодательства об общественном контроле. Первая часть указанной статьи содержит общие положения, наделяющие субъектов общественного контроля вносить в компетентные органы предложения о привлечении виновных должностных лиц органов государственной власти и органов местного самоуправления к ответственности в случае нарушения прав и свобод человека и гражданина, прав и законных интересов общественных объединений и иных негосударственных некоммерческих организаций.

В части 2 ст. 27 Федерального закона введено общее основание ответственности физических и юридических лиц - воспрепятствование законной деятельности субъектов общественного контроля. В федеральных законах, Кодексе Российской Федерации об административных правонарушениях и Уголовном кодексе Российской Федерации не содержится санкций за воспрепятствование законной деятельности субъектов общественного контроля. Поэтому в развитие Федерального закона об общественном контроле указанные федеральные законы нуждаются в дополнениях.

Нормы ФЗ «Об основах общественного контроля в РФ» должны стать отправной точкой и «дорожной картой» для совершенствования текущего законодательства в данной сфере в плане восполнения пробелов и преодоления противоречий. Формируя законодательную основу осуществления общественного контроля, государство создает прочный фундамент для построения эффективного правового государства и формирования зрелого гражданского общества.

Реализация ФЗ повысит степень доверия общества к власти. Данное утверждение справедливо как для отношения граждан к центральной власти, так и к органам местного самоуправления, что будет способствовать проведению эффективных реформ и преобразований в российском обществе [6].

Совершенствуя законодательство в сфере общественного контроля, необходимо продолжать разрабатывать концепцию общественного контроля, отражающую тенденцию усиления влияния гражданского общества на деятельность государства. Органам государственной власти и местного самоуправления следует продолжать работу по повышению правовой грамотности граждан и повышению их социально-правовой активности, чтобы стать деятельными участниками осуществления различных форм общественного контроля.

Список литературы

- [1]. *Гриб В.В.* Общественный контроль: учебник. – М.: ИГ «Юрист», 2017. – 656 с.
- [2]. *Гегель Г.В.Ф.* Философия права. – М.: Изд-во «Мысль», 1996. – 524 с.
- [3]. *Панарин А.С.* Глобальное политическое прогнозирование. – М. – 2002. – 295 с..
- [4]. *Лучин В.О., Боброва Н.А.* Конституционный строй России: основные политико-правовые характеристики // Право и политика. – 2003. – № 10. – С. 24-27.
- [5]. *Федеральный закон от 21.07.2014 № 212-ФЗ «Об основах общественного контроля в Российской Федерации» //* Собрание законодательства РФ. – 2014. – № 30 (ч. 1). – Ст. 4213.
- [6]. *Гриб В.В.* Актуальные проблемы правового развития института общественного контроля в Российской Федерации // Конституционное и муниципальное право. – 2015. – № 11. – С. 3–13.
- [7]. *Послание Президента Российской Федерации Федеральному Собранию Российской Федерации //* Российская газета. – 2005. – от 26 апр.

[8]. *Струсь К.А.* Государство и гражданское общество: проблемы правового взаимодействия в России. – Саратов. – 2003.

Шафигуллина Татьяна Владимировна – доцент, канд. ист. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: tania56_09@mail.ru

Стадникова Ирина Дмитриевна – студентка КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: irin1999@yandex.ru

ОСНОВНЫЕ ПРАВА ГОСУДАРСТВЕННЫХ ИНСПЕКТОРОВ ТРУДА

Конституция РФ гарантирует государственную защиту прав и свобод человека, а значит, и трудовых прав работников [1].

В числе основных принципов правового регулирования труда Трудовой кодекс РФ (далее – ТК РФ) называет обеспечение прав каждого на защиту государством его трудовых прав и свобод (ч.1 ст.1). Этот принцип конкретизирован в главах 57 и 58 раздела XIII ТК РФ, посвященного защите трудовых прав работников [2].

Проблема защищенности трудовых прав – одна из насущных проблем. Работники редко изъявляют желание бороться за свои права, опасаясь потерять работу, работодатель нередко этим пользуется.

Ключевая роль в защите прав работников и трудового законодательства отводится инспекторам государственной инспекции труда.

Права, обязанности и ответственность государственных инспекторов труда закреплены ТК РФ, Федеральным законом «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (далее – Закон № 294-ФЗ) [3]. Однако необходимо учитывать, что для регулирования их деятельности применяются и международные договоры, ратифицированные Российской Федерацией [4].

Статья 357 ТК РФ устанавливает основные права государственных инспекторов труда, позволяющие выявлять факты нарушений трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права, работодателями и их представителями и фиксировать обстоятельства, способствующие правонарушениям.

В целях обеспечения защиты трудовых прав работников государственные инспекторы труда наделены правом беспрепятственно в любое время суток посещать инспеклируемые организации всех организационно-правовых форм и форм собственности.

В порядке реализации предоставленных полномочий в течение 2017 года государственными инспекциями труда было организовано и проведено 148,9 тыс. проверок по вопросам соблюдения законодательства о труде, в том числе 134,8 тыс. внеплановых проверок. Из общего количества проведенных проверок в плановом порядке проведено более 14 тыс. проверок или 9,4%, тогда как остальные проверки (90,6%) проводились во внеплановом порядке [5].

Анализ результатов надзорной деятельности государственных инспекций труда в субъектах Российской Федерации свидетельствует, что причинами и условиями сохраняющейся массовости нарушений трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права, на протяжении последних лет является:

- неудовлетворительное экономическое, финансовое и технологическое состояние большого числа хозяйствующих субъектов, низкий уровень производительности труда и конкурентоспособности выпускаемой продукции;
- сокращение финансирования и материально-технического обеспечения мер по безопасности производства и охране труда;
- несоответствие локальных актов, принимаемых работодателем трудовому законодательству (отсутствие в трудовых договорах работников обязательных условий: условия оплаты труда, режима труда и отдыха, даты начала работы, характеристик условий труда);
- ненадлежащее осуществление внутриведомственного и регионального контроля за соблюдением законодательства о труде и охране труда со стороны федеральных министерств и ведомств, органов исполнительной власти субъектов Российской Федерации и местного самоуправления, а также самих работодателей на предприятиях и в организациях.

Для прохода государственного инспектора на территорию проверяемой организации ему достаточно предъявить служебное удостоверение установленного образца.

Государственный инспектор труда имеет право на месте знакомиться с документами и материалами, чтобы получить необходимую информацию. При этом недопустимо уклонение работодателей и их представителей от представления документов под каким-либо предлогом, в т. ч. по мотивам содержания в них коммерческой или государственной тайны.

Госинспектор вправе знакомиться со всеми документами, которые могут содержать информацию о нарушении трудовых прав работников. В их число входят: приказы и распоряжения, статистическая отчетность, акты проверок работы подведомственных организаций, письма, жалобы и предложения граждан по вопросам, относящимся к компетенции проверяемого органа, и др. В случае необходимости государственный инспектор труда вправе обратиться с просьбой об изготовлении для него копий отдельных документов.

В целях наиболее полной проверки государственные инспекторы труда направляют контролируемым органам соответствующие письма (запросы) с конкретным указанием необходимых для представления материалов.

Недопустим отказ работодателей (их представителей) предоставить необходимую информацию на том основании, что она не может быть безвозмездной.

В отношении нарушителей ст. 357 ТК РФ о безвозмездности представления государственному инспектору труда необходимой информации он должен использовать все имеющиеся в его распоряжении средства воздействия [2].

Актом реагирования государственного инспектора труда на нарушения, выявленные в ходе проверки, является предписание об устранении вскрытых правонарушений, их причин и способствующих им условий.

Предписание составляется в 2 экземплярах и оформляется в соответствии с требованиями, указанными в ст. 9 Закона № 294-ФЗ [3].

Один экземпляр предписания с копиями приложений (протоколы проведенных исследований и экспертиз, объяснения работников) вручается работодателю или его представителю под расписку либо направляется по почте с уведомлением о вручении, которое приобщается к экземпляру предписания, остающемуся в деле проверяющего органа федеральной инспекции труда.

Содержащиеся в предписании рекомендации должны иметь правовую направленность и не касаться оперативно-хозяйственной деятельности проверяемой организации.

В предписании допустима постановка вопроса о необходимости привлечения руководителей и иных должностных лиц организации к дисциплинарной ответственности или об отстранении их от работы.

Выполнение предписаний государственных инспекторов труда является обязанностью работодателя, возложенной на него ст. 212 ТК РФ.

За неисполнение в установленный срок предписания государственного инспектора труда об устранении нарушений законодательства предусмотрена административная ответственность. Государственные инспекторы труда имеют право составлять протоколы об административных правонарушениях, предусмотренных ч. 2 ст. 5.27; ст. 5.42; ч. 1 ст. 19.4; ч. 1 ст. 19.5; ст. 19.6; 19.7 КоАП.

Государственными инспекторами труда в 2017 г. наложено 101,85 тыс. штрафов на общую сумму почти 574 млн. руб.

В судебные органы направлено 8,8 тыс. протоколов о привлечении к административной ответственности, в том числе 324 протокола о дисквалификации должностных лиц. По результатам их рассмотрения судами принято 5,7 тыс. решений об административных наказаниях виновных лиц, включая дисквалификацию 174 руководителей различных уровней [5].

В ходе проведенных проверок всех видов и расследований несчастных случаев на производстве государственными инспекторами труда было выявлено более 846 тыс. нарушений трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права, из них более 540 тыс. нарушений законодательства об охране труда.

Обязанность проходить обучение об охране труда и проверку знаний требований охраны труда в соответствии ст. 225 ТК РФ, возложена на всех работников организаций, включая руководителей.

Государственные инспекторы труда наделены правом выдавать предписания об отстранении от работы лиц, не прошедших в установленном порядке обучение безопасным методам и приемам выполнения работ, инструктаж по охране труда, стажировку на рабочих местах и проверку знания требований охраны труда.

Почти 67 тыс. работников не прошли своевременно в установленном порядке обучение, инструктаж и проверку знаний по охране труда и были отстранены от работы [5].

В интересах обеспечения безопасных условий труда в 2017 г. прекращена эксплуатация свыше 92,7 тыс. единиц средств индивидуальной защиты, не имевших сертификатов и не соответствовавших требованиям охраны труда [5].

В тех случаях, когда действия работодателя и его представителей содержат признаки деяния, наказуемого в уголовном порядке, государственные инспекторы труда могут направлять в правоохранительные органы материалы о привлечении указанных лиц к уголовной ответственности.

По результатам проведенных проверок, к дисциплинарной ответственности привлечено около 9 тыс. должностных лиц, возбуждено 287 уголовных дел [5].

В 2017 году государственными инспекциями труда рассмотрено более 459 тыс. обращений граждан. Основной причиной для направления в федеральную инспекцию труда обращений граждан являлись: невыплата долгов по заработной плате (более 39,6%). Более 21% обращений содержали сведения о несоблюдении установленных требований при оформлении либо расторжении трудовых отношений.

В порядке оказания гражданам правовой помощи по вопросам трудового законодательства должностными лицами федеральной инспекции труда была оказана помощь в подготовке 6 177 судебных исков, из которых судом было удовлетворено 1 429 случаев [5].

Проблемами, оказывающими негативное влияние на эффективность правоприменительной деятельности, и существенно ограничивающими возможность должностных лиц, уполномоченных на осуществление федерального государственного надзора за соблюдением трудового законодательства, оперативно находить и правильно применять необходимые нормы права продолжают оставаться:

- отсутствие должной систематизации трудового законодательства, включая законодательство об охране труда;
- неопределенность правового регулирования, вызванная: наличием в трудовом праве пробелов и коллизий, а также отсутствием подкрепления отдельных норм Трудового кодекса РФ;
- непринятие уполномоченными органами государственной власти нормативно-правовых актов в развитие бланкетных норм ТК РФ [5].

В условиях реформирования общественных отношений необходимо постоянно совершенствовать механизм правовой защиты работающих.

Правовое регулирование трудовых отношений должно соответствовать характеру структурных преобразований в экономике как по форме, так и по содержанию.

Список литературы

- [1]. *Конституция Российской Федерации* (принята всенародным голосованием 12.12.1993) (с учетом поправок от 21.07.2014 № 11-ФКЗ) // СЗ РФ. – 04.08.2014. – № 31. – ст. 4398.

[2]. *Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ // СЗ РФ от 7 января 2002 г. – № 1 (часть I) ст. 3.*

[3]. *Федеральный закон от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» [Электронный ресурс]. URL: <http://www.rg.ru/2008/12/30/prava-kontrol-dok.html>*

[4]. *Федеральным законом от 11.04.1998 № 58-ФЗ О ратификации Конвенции 1947г. № 81 «Об инспекции труда в промышленности и торговле» // СЗ РФ. – 1998. – № 15. – ст. 1698*

[5]. *Доклад об осуществлении и эффективности федерального государственного надзора за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права. [Электронный ресурс]. URL: <http://www.rostrud.ru/activities/28/otchet/>*

Карпов Максим Алексеевич – студент КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: karповmaksim.ru@mail.ru

Титков А.А. –

Шафигуллина Татьяна Владимировна – доцент, канд. ист. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: tania56_09@mail.ru

И.Д. Стадникова, И.С. Азаренко

СНВ-3: БУДЕТ ЛИ ПРОЛОНГАЦИЯ?

Ядерной войной принято называть гипотетическое столкновение между странами или военно-политическими блоками, имеющими термоядерное или ядерное оружие и пустившими его в действие. История ядерной войны, к счастью, пока не написана. До последнего времени считалось, что это страшное оружие является оружием сдерживания. Однако реалии сегодняшнего дня остро поставили вновь, как во время Карибского кризиса, угрозу ядерной мировой катастрофы. Попробуем разобраться, в чем острота ситуации.

Наиболее важную роль в данном вопросе играют взаимоотношения между Россией и Соединенными Штатами Америки. Гонка вооружений между странами привела к необходимости создания серии двусторонних договоров между странами об ограничениях стратегических ядерных сил.

Первым таким договором был ОСВ-I, подписанный в 1972 году и закрепивший количество средств доставки ядерного оружия для каждой из сторон на том уровне, на каком они находились в тот момент. Однако к этому времени и в СССР, и в США уже начали оснащать ракеты разделяющимися головными частями с блоками индивидуального наведения. В результате именно в период разрядки начался невиданный прежде, лавинообразный процесс наращивания ядерного потенциала. Договор также предусматривал принятие на вооружение новых баллистических ракет, размещаемых на подводных лодках, строго в том количестве, в котором были ранее списаны устаревшие баллистические ракеты наземного базирования.

СНВ-3 стал седьмым в серии договоров. Это двусторонний договор между Россией и Соединёнными Штатами относительно дальнейшего взаимного сокращения арсеналов развернутых стратегических ядерных вооружений. Этот договор заменил истекший СНВ-1, подписанный в июле 1991 года Михаилом Горбачевым и Джорджем Бушем (СНВ-2 был позднее подписан Борисом Ельциным и Биллом Клинтонем, но в силу так и не вступил). Договор был подписан президентами Дмитрием Медведевым и Барак Обама 8 апреля 2010 года в Праге, вступил в силу 5 февраля 2011 года и истекает в феврале 2021 года.

СНВ-3 – это главный договор, который сейчас удерживает Россию и США от гонки ядерных вооружений. Согласно ему Россия и США сократили свои ядерные арсеналы так, чтобы суммарные количества вооружений не превышали 700 межконтинентальных баллистических ракет, баллистических ракет на подводных лодках и стратегических бомбардировщиках, а также 1550 боеголовок и 800 развернутых и неразвернутых пусковых установок.

Однако за прошедшие года отношения между двумя странами стали заметно хуже: США ввели санкции против России, а переговоры по многим вопросам между ними заходят в тупик.

США требуют, чтобы к договору присоединился Китай. Россия считает, что в нем тогда могли бы участвовать и Великобритания с Францией, чьи ядерные потенциалы соизмеримы с китайским.

Второе условие американцев – включение в договор нестратегических ядерных вооружений России. Наконец, третье условие – создание более эффективного механизма проверки ядерного арсенала.

Россия считает, что договор можно было бы продлить и без изменения действующего механизма.

Эксперт Российского совета по международным делам Илья Крамник полагает, что если договор все-таки не будет продлен, то Россия при этом постарается не менять свой ядерный потенциал – по крайней мере, количественно.

«При снижении количества зарядов, которое у нас есть, стабильность начинает размываться, потому что возникает риск обезоруживающего удара, в том числе и с использованием обычных вооружений. А в обычных вооружениях США и НАТО нас существенно превосходят», – сказал он.

По его мнению, свертывание контроля над вооружениями «открывает новую эпоху стратегических взаимоотношений между США и Россией, в которой развитие ядерных вооружений не будет регулироваться международными соглашениями». Он прогнозирует, что недоверие между двумя странами будет расти и дальше, что может привести к новой гонке вооружений.

Шестнадцатого октября президент России Владимир Путин предложил Вашингтону продлить действующий Договор СНВ-3 без всяких предварительных условий «хотя бы на год», чтобы иметь возможность провести содержательные переговоры по всем параметрам». В МИД РФ 20 октября заявили, что Москва предлагает продлить СНВ-3 на один год и при этом готова вместе с США взять на себя политическое обязательство, чтобы заморозить на данный период количество имеющихся у сторон ядерных боезарядов при условии, что если решение о такой взаимной «заморозке» будет достигнуто, то оно не должно сопровождаться никакими дополнительными требованиями со стороны США.

В свою очередь, Роберт О'Брайен тогда критически оценил предложение российской стороны, однако впоследствии добавил, что Белый дом официально ответит на эту инициативу.

Самой крупной потерей в случае окончания действия СНВ-3 будет утрата информации, получаемой по механизму верификации. Дважды в год стороны обмениваются огромным объемом информации, включая расположение каждой ракеты, количество боеголовок, дату производства, перемещение и статус. Если этих данных не будет, это помимо прочего заставит обе стороны при военном планировании чаще исходить из худших сценариев.

Очевидно, что администрация Трампа рассчитывает извлечь геополитические дивиденды при любом сценарии развития переговоров. При том надо отметить, что здравые голоса и в Америке раздаются. Так экспертное американское сообщество поддерживает пролонгацию, американские наблюдатели называют «подключение» к соглашению Китая нереалистичным. Америку

ждут выборы, так что призрачная надежда на положительный исход ситуации все-таки есть.

Угроза не пролонгации СНВ-3 создает реальные предпосылки для разрушения глобального режима стратегической стабильности в настоящее время, что может привести к непредсказуемым последствиям. Очень хочется надеяться на здравый смысл, однако время покажет... .

Список литературы

[1]. *Плюсы и минусы Российско-американских соглашений / Россия в глобальной политике.* URL: <https://globalaffairs.ru/articles/dogovor-po-snv-imperativ-zhestkoj-sily/> (дата обращения 22.10.20).

[2]. *Договор об СНВ между Россией и США: будущее туманно/BBCNews . Русская служба.* URL: <https://www.bbc.com/russian/features-42947145> (дата обращения 22.10.20).

Азаренко Инна Сергеевна – старший преподаватель, канд. техн. наук КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: 89108651131@mail.ru

Стадникова Ирина Дмитриевна – студентка КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия. E-mail: irin1999@yandex.ru

СОДЕРЖАНИЕ

СЕКЦИЯ 8.	
ЗАЩИТА ИНФОРМАЦИИ	3
1. К.Ю. Войцев	
АЛГОРИТМ СОЗДАНИЯ QR-КОДА.....	4
2. А.А. Бабкин, И.В. Глебов	
АНАЛИЗ ЗАЩИЩЕННОСТИ И УЯЗВИМОСТЕЙ ИГРОВЫХ ДВИЖКОВ.....	8
3. П.Р. Курдюков, А.Б. Лачихина	
АНАЛИЗ ЗАЩИЩЁННОСТИ ИНФОРМАЦИИ, ЗАКОДИРОВАННОЙ В QR-КОДЕ, И МЕХАНИЗМОВ ЗАСЕКРЕЧИВАНИЯ ИНФОРМАЦИИ	13
4. В.В. Драган	
АНАЛИЗ МЕТОДОВ ВЕРИФИКАЦИИ БЕЗОПАСНОСТИ ПО	15
5. Я.А. Кадурин	
АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИКОСМИЧЕСКИХ АППАРАТОВ.....	20
6. Е.Ю. Шестопалов, А.Н. Молчанов	
АНАЛИЗ ПРОГРАММНЫХ ЛОГОВ.....	25
7. А.И. Самохина	
АНАЛИЗ ПРОГРАММНЫХ ПРОДУКТОВ ДЛЯ УДАЛЁННОГО КОНТРОЛЯ ИСПОЛНЯЕМЫХ ПРОЦЕССОВ НА РАБОЧИХ СТАНЦИЯХ	29
8. Д.Д. Теренин, А.Б. Лачихина	
АНАЛИЗ СРАВНИТЕЛЬНОЙ ЭФФЕКТИВНОСТИ ПРОГРАММНЫХ ПРОДУКТОВ ТЕСТИРОВАНИЯ УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ.....	34
9. Е.М. Бандурина, И.И. Ерохин	
БЕЗОПАСНОСТЬ ДАТА-ЦЕНТРА: ФИЗИЧЕСКИЙ И ЦИФРОВОЙ УРОВНИ ЗАЩИТЫ	38
10. Е.М. Бандурина, И.И. Ерохин	
ИЗМЕРЕНИЕ КИБЕРФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ В ПРОМЫШЛЕННЫХ СИСТЕМАХ УПРАВЛЕНИЯ С ПОМОЩЬЮ СТРАТЕГИЙ АТАК С МИНИМАЛЬНЫМИ УСИЛИЯМИ.....	41
11. Е.В. Поддубная	
ИНФОРМАЦИОННАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ ЧЕЛОВЕЧЕСКИМИ РЕСУРСАМИ ПРЕДПРИЯТИЯ ТРАНСПОРТИРОВКИ ГАЗА	45
12. М.Д. Романкин, А.Б. Лачихина	
ИССЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ СИСТЕМЫ ТЕХНИЧЕСКОЙ ПОДГОТОВКИ ПРОИЗВОДСТВА	48

13. Е.С. Еськов	
ИССЛЕДОВАНИЕ МЕТОДОВ КОНТРОЛЯ МОБИЛЬНЫХ УСТРОЙСТВ НА БАЗЕ ANDROID	51
14. П.Ю. Малахов, А.Б. Лачихина	
КУЛЬТУРА ОБОРОТА ПЕРСОНАЛЬНЫХ ДАННЫХ РОССИЙСКОГО СЕКМЕНТА ИНТЕРНЕТА	54
15. А.М. Волков, П.Д. Каян, С.В. Козин	
О ВАЖНОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РЕАЛИЯХ 2020 ГОДА	57
16. С.Е. Липатова, Ю.Е. Гагарин	
ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ KUBERNETES	59
17. А.Р. Филатов	
ОБЗОР АЛГОРИТМОВ РАСПОЗНАВАНИЯ ЛИЦ, ПРИМЕНЯЕМЫХ ДЛЯ АУТЕНТИФИКАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ	64
18. И.Е. Рунов	
ОБЗОР СУЩЕСТВУЮЩИХ АЛГОРИТМОВ РАСПОЗНАВАНИЯ ЛИЦ	67
19. Е.М. Бандурина, И.И. Ерохин	
ОБОСНОВАНИЕ ВЫБОРА НЕКОНТРОЛИРУЕМЫХ АЛГОРИТМОВ С ПОМОЩЬЮ АТАК И КЛАССОВ АНОМАЛИЙ	71
20. М.Г. Шеленкова	
ОБРАТИМОЕ СКРЫТИЕ ДАННЫХ ДЛЯ ДВОИЧНЫХ ИЗОБРАЖЕНИЙ	74
21. Е.М. Бандурина, Ю.Е. Гагарин	
ОПРЕДЕЛЕНИЕ ТИПОВ ФИШИНГОВЫХ АТАК И МЕТОДЫ ИХ ПРЕДОТВРАЩЕНИЯ	78
22. А.А. Артемова, А.А. Литвиненко, И.И. Ерохин	
ПРИМЕНЕНИЕ АВТОМАТИЧЕСКОГО СКАНЕРА ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ СЕТИ	81
23. А.А. Сальникова, С.М. Твердова	
СРЕДСТВА И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА	85
24. И.И. Ерохин, Д.В. Климущина	
ТЕХНОЛОГИЯ DLP	87
25. Е.М. Бандурина, И.И. Ерохин	
ТРЕХФАКТОРНАЯ АНОНИМНАЯ СХЕМА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ СРЕД ИНТЕРНЕТА ВЕЩЕЙ	92

**СЕКЦИЯ 9.
ДИНАМИКА, ПРОЧНОСТЬ И НАДЕЖНОСТЬ
ПОДЪЕМНО-ТРАНСПОРТНЫХ, СТРОИТЕЛЬНЫХ,
ДОРОЖНЫХ МАШИН И ОБОРУДОВАНИЯ 95**

1. И.И. Сорокина

К ВОПРОСУ ПРОЕКТИРОВАНИЯ ОРТОГОНАЛЬНОЙ ЧЕРВЯЧНОЙ
ПЕРЕДАЧИ С КОСОЗУБЫМ ЦИЛИНДРИЧЕСКИМ КОЛЕСОМ 96

2. В.В. Моргунов, П.В. Витчук

МЕТОД РАСШИФРОВКИ КАНАТА И ОЦЕНКИ ЕГО ПРОЧНОСТИ..... 98

3. А. Г. Черенков

УНИВЕРСАЛЬНАЯ МАШИНА
ДЛЯ ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ АВАРИЙ..... 102

**СЕКЦИЯ 10.
МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И ФИЗИКО –
МАТЕМАТИЧЕСКИЕ ПРОБЛЕМЫ ПРОЕКТИРОВАНИЯ
СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ 106**

1. П.Е. Белоножко, Ю.Е. Гагарин

ИСПОЛЬЗОВАНИЕ МЕТОДА АНАЛИЗА СЕТИ ДЛЯ РЕШЕНИЯ ЗАДАЧИ О
МНОГОПОЛЮСНОМ МАКСИМАЛЬНОМ ПОТОКЕ 107

2. Е.Д. Мосин, Ю.Е. Гагарин

ПРИМЕНЕНИЕ МЕТОДА РАССТАНОВКИ ПОМЕТОК ДЛЯ НАХОЖДЕНИЯ
МАКСИМАЛЬНОГО ПОТОКА 111

**СЕКЦИЯ 12.
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ.
ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫЕ МАШИНЫ 114**

1. Ю.Е. Гагарин, Д.В. Климушина

5G-СВЯЗЬ И ЕЁ ХАРАКТЕРИСТИКА 115

2. К.А. Тронов, Е.В. Красавин

ИОТ И ТУМАННЫЕ ВЫЧИСЛЕНИЯ 120

3. А.М. Булкина, А.В. Максимов

АНАЛИЗ АППАРАТНОЙ РЕАЛИЗАЦИИ ОПЕРАЦИИ УМНОЖЕНИЯ
КВАТЕРНИОНОВ 125

4. Е.В. Красавин, В.О. Трешневская

ВЫБОР ПЛАТФОРМЫ ДЛЯ ВЕБИНАРОВ В ЛОКАЛЬНЫХ СЕТЯХ:
МАСШТАБИРУЕМОСТЬ, ПРОСТОТА, БЕЗОПАСНОСТЬ..... 130

5. Н.А. Гаранин, Е.В. Красавин

ИНТЕРНЕТ ВЕЩЕЙ ИОТ. ПРОТОКОЛЫ 134

6. К.А. Жидков, Е.В.Красавин	
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОТСЛЕЖИВАНИЯ МЕСТОПОЛОЖЕНИЯ И ИХ ИСПОЛЬЗОВАНИЕ В СИСТЕМЕ «УМНЫЙ ГОРОД»	138
7. Ю.Ю. Сарычева, Е.В. Красавин, В.О.Трешневская	
ИСПОЛЬЗОВАНИЕ СЕТЕЙ ДАЛЬНОГО РАДИУСА ДЕЙСТВИЯ И ЗАЩИТА УЗЛОВ СИСТЕМЫ УМНОГО ГОРОДА	141
8. А.В. Дунаев, В.В. Сергеев	
СРАВНЕНИЕ ВИРТУАЛИЗАЦИИ И КОНТЕЙНЕРИЗАЦИИ.....	145
9. М.В. Зейкан, Е.Д. Гуркина	
ОБЗОР ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ, ПРЕИМУЩЕСТВ И НЕДОСТАТКОВ СЕРВИСОВ ПО ПРОДАЖЕ И ДОСТАВКЕ ПИЦЦЫ.....	147
10. А.С. Рязанцев, Е.Д. Гуркина	
ОБОСНОВАНИЕ ВЫБОРА ИНСТРУМЕНТОВ И ТЕХНОЛОГИЙ АРМ ПРИ ПРОЕКТИРОВАНИИ ПРИЛОЖЕНИЯ ДЛЯ ВОСПИТАТЕЛЯ ДЕТСКОГО САДА	150
11. М.И. Силкин, Е.Д. Гуркина	
ОБОСНОВАНИЯ ВЫБОРА ИНСТРУМЕНТОВ И ТЕХНОЛОГИЙ РАЗРАБОТКИ СЕРВЕРНЫХ ЧАСТЕЙ ИГРОВЫХ ПРИЛОЖЕНИЙ	153
12. В.В. Сергеев, А.В. Дунаев	
ОБУЧЕНИЕ НЕЙРОННОЙ СЕТИ ДЛЯ ПОИСКОВОГО ЧАТ-БОТА.....	157
13. А.В. Бояровская, Н.А. Борсук	
ОСНОВНЫЕ ЭТАПЫ ПЕРЕХОДА ИЗ СИСТЕМЫ КАДРОВОГО И БУХГАЛТЕРСКОГО УЧЕТА «А1-ПЕРСОНАЛ» В СИСТЕМУ «1С».....	161
14. Г.П. Макаров, Е.В. Вершини	
ПРИМЕНЕНИЕ ТЕХНОЛОГИИ DNSOVERHTTPS В ЦЕЛЯХ ЗАЩИТЫ ОТ ИНФОРМАЦИОННЫХ АТАК	164
15. А.А. Разгоев, Ю.Е.Гагарин	
ПРОЕКТИРОВАНИЕ УСТРОЙСТВА ДЛЯ ДОМАШНЕГО ТЕРМОСТАТИРОВАНИЯ	167
16. А.А.Петрушин, И.В. Чухраев	
РАЗРАБОТКА ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В МОДУЛЕ ОБНАРУЖЕНИЯ СТОРОННИХ ПРЕДМЕТОВ В СИСТЕМЕ АВТОДОСМОТРА	170
17. С.Д. Кургузов, В.А. Гартман, Н.А. Борсук	
РАЗРАБОТКА МОДУЛЯ АВТОРИЗАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ДЛЯ СТУПЕНЕЙ НАЧАЛЬНОЙ ШКОЛЫ.....	172

18. Г.А. Коротков	
АВТОМАТИЗАЦИЯ В МАШИННОМ ОБУЧЕНИИ	176
19. Н.А. Пильщиков, Е.О. Дерюгина, И.В. Чухраев	
ИССЛЕДОВАНИЕ ПЛАТФОРМ ДЛЯ ДИСТАНЦИОННОГО ОБУЧЕНИЯ	181
20. М.И. Колосов, И.В. Чухраев	
ХАРАКТЕРИСТИКА И СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЯЗЫКА ПРОГРАММИРОВАНИЯ GOLANG	184

СЕКЦИЯ 14.

ИННОВАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ И НАУЧНО-МЕТОДИЧЕСКИЕ ВОПРОСЫ ВНЕДРЕНИЯ РЕЗУЛЬТАТОВ НИР В УЧЕБНЫЙ ПРОЦЕСС

187

1. Л.С. Беккель	
ИСПОЛЬЗОВАНИЕ UNITY ДЛЯ РАЗРАБОТКИ ПРИЛОЖЕНИЙ ВИРТУАЛЬНОЙ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ	188
2. В.В. Сахаров	
МОТИВАЦИЯ СТУДЕНТОВ НА ЗАНЯТИЯХ ПО ИНЖЕНЕРНОЙ ГРАФИКЕ	190
3. О.В. Сулина, Е.А. Шестернина	
РЕОРГАНИЗАЦИЯ КУРСА ДИСЦИПЛИНЫ НАЧЕРТАТЕЛЬНАЯ ГЕОМЕТРИЯ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ	194
4. А.Д. Аксенов, Е.Н. Сломинская	
РОЛЬ ИНЖЕНЕРНО-ГРАФИЧЕСКИХ ДИСЦИПЛИН В ПОДГОТОВКЕ БАКАЛАВРОВ ПО НАПРАВЛЕНИЮ ИННОВАТИКА	196
5. А.Р. Крицкая, Т.С. Китаева	
САМОСТОЯТЕЛЬНАЯ РАБОТА КАК МЕТОДИЧЕСКАЯ ОСНОВА САМООБРАЗОВАНИЯ ОБУЧАЮЩИХСЯ В КОНТЕКСТЕ НЕПРЕРЫВНОГО ОБРАЗОВАНИЯ	199
6. Н.Е. Зайчиков, А.М. Зув	
СПОСОБЫ ПОСТРОЕНИЯ ЭЛЛИПСА	203

СЕКЦИЯ 15.

СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ЭКОНОМИКИ

210

1. Т.Ш. Полякова	
ПРОБЛЕМЫ ОРГАНИЗАЦИИ ПРОИЗВОДСТВА В ПЕРИОД ПАНДЕМИИ	211
2. А.В. Челенко	
РОЛЬ ТЕХНОЛОГИЧЕСКИХ ИННОВАЦИЙ В ЭКОНОМИКЕ ШЕСТОГО ИНДУСТРИАЛЬНОГО УКЛАДА	214

3. **С.Ю. Иванов, И.В. Неклюдова, В.В. Квашина**
СУЩНОСТЬ ПОЛИТИКИ КОНКУРЕНТОСПОСОБНОСТИ,
ОСОБЕННОСТИ ФОРМИРОВАНИЯ И МЕХАНИЗМЫ ЕЁ РЕАЛИЗАЦИИ 219

4. **А.Д. Кузнецова**
ЭКОНОМИКА РОССИИ ВО ВРЕМЯ ПАНДЕМИИ КОРОНАВИРУСА
И МЕТОДЫ ПОДДЕРЖКИ БИЗНЕСА 222

СЕКЦИЯ 16.

ОБЩЕСТВЕННО-ПОЛИТИЧЕСКИЕ И ФИЛОСОФСКИЕ ВОПРОСЫ РАЗВИТИЯ ОБЩЕСТВА.....224

1. **И.С. Азаренко, Ю.В. Егоренкова**
КАРАБАХ С НОВА В ОГНЕ: ПОЧЕМУ СЕГОДНЯ?! 225

2. **И.Д. Стадникова, Т.В. Шафигуллина**
ОБЩЕСТВЕННЫЙ КОНТРОЛЬ: ЗАКОНОДАТЕЛЬНОЕ ЗАКРЕПЛЕНИЕ 228

3. **М.А. Карпов, А.А. Титков, Т.В. Шафигуллина**
ОСНОВНЫЕ ПРАВА ГОСУДАРСТВЕННЫХ ИНСПЕКТОРОВ ТРУДА 235

4. **И.Д. Стадникова, И.С. Азаренко**
СНВ-3:БУДЕТ ЛИ ПРОЛОНГАЦИЯ? 240

**НАУКОЕМКИЕ ТЕХНОЛОГИИ
В ПРИБОРО- И МАШИНОСТРОЕНИИ
И РАЗВИТИЕ ИННОВАЦИОННОЙ
ДЕЯТЕЛЬНОСТИ В ВУЗЕ**

**Материалы
Всероссийской научно-технической конференции**

Том 2

Научное издание

Все работы публикуются в авторской редакции. Авторы несут ответственность за подбор и точность приведенных фактов, цитат, статистических данных и прочих сведений

Подписано в печать 27.11.2019
Формат 60x90/16. Печать офсетная. Бумага офсетная. Гарнитура «Таймс»
Печ. л. 15,63. Усл. п. л. 14,53

Издательство МГТУ им. Н.Э. Баумана
107005, Москва, 2-я Бауманская, 5

Оригинал-макет подготовлен в Редакционно-издательской группе
отдела научной инновационной деятельности
КФ МГТУ им. Н.Э. Баумана
248000, г. Калуга, ул. Баженова, 2, тел. 57-31-87