ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 4(26) / 2017

УЧРЕДИТЕЛИ

ФГБОУ ВПО «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ООО «ЮЖНО-УРАЛЬСКИЙ ЮРИДИЧЕСКИЙ ВЕСТНИК»

ГЛАВНЫЙ РЕДАКТОР

ШЕСТАКОВ А. Л.,
д. т. н., профессор, ректор ФГАОУ ВО «ЮУрГУ (НИУ)» (г. Челябинск)

ОТВЕТСТВЕННЫЙ РЕДАКТОР

РАДИОНОВ А. А.,
д. т. н., профессор, проректор ФГАОУ ВО «ЮУрГУ (НИУ)» (г. Челябинск)

ВЫПУСКАЮЩИЙ РЕДАКТОР

СОГРИН Е. К.

ВЁРСТКА

ШРЕЙБЕР. А. Е.

КОРРЕКТОР

ФЁДОРОВ. В. С.

Журнал «Вестник УрФО. Безопасность в информационной сфере» включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство ПИ № ФС77-65765 от 20.05.2016

Издатель: **ООО «Южно-Уральский юридический вестник»**

Адрес редакции и издателя: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.
Тел./факс (351) 267-97-01.

Электронная версия журнала в Интернете:
www.info-secur.ru,
e-mail: urvest@mail.ru

16+

ISSN 2225-5435

UrFR Newslette
INFORMATION SECURITY
№ 4(26) / 2017

FOUNDER

SOUTH URAL STATE UNIVERSITY

SOUTH URAL LEGAL NEWSLETTER

CHIEF EDITOR

SHESTAKOV A. L.,
doctor of Technical Sciences, Professor, Rector South Ural State University, (Chelyabinsk)

MANAGING EDITOR

RADIONOV A. A.,
Doctor of Technical Sciences, Professor, Vice-Rector South Ural State University, (Chelyabinsk

PRODUCING EDITOR

SOGRIN E. K.

LAYOUT

SHRABER. A. E.

PROOFREADING

FEDOROV. V. S.

The journal « UrFR Newsletter. Information Security » is included in the List peer-reviewed scientific publications, in which should be published main scientific results of scientific dissertations degree of doctor and candidate of science

Subscription index 73852

in the «Russian Post» catalog

The journal is registered by the Federal service in the field of communication, information technology and mass communications.

Certificate
PI No. ФС77-65765 dd. 05/20/2016

Publisher: OOO « South Ural Legal Newsletter»

Editorial and publisher address: Russia, 454080, Chelyabinsk, Lenin Avenue, 76
Phone / fax (351) 267-97-01.

Electronic version of the magazine in the Internet:

www.info-secur.ru,
e-mail: urvest@mail.ru

16+

В НОМЕРЕ

ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

ОРГАНИЗАЦИОННАЯ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

ПРАКТИЧЕСКИЙ АСПЕКТ

TECHNICAL MEANS AND METHODS OF INFORMATION PROTECTION

ORGANIZATIONAL AND ORGANIZATIONAL - TECHNICAL PROTECTION OF INFORMATION

ACTUAL PROBLEMS OF CYBERSECURITY

LEGAL REGULATION OF INFORMATION SECURITY

THE PRACTICAL ASPECT

УДК 004.93.056 + 004.7.056 Вестник УрФО № 4(26) / 2017, с. 5–8

Сарайкин М. А., Борисов А. П.

РАЗРАБОТКА СИСТЕМЫ БИОМЕТРИЧЕСКОЙ ЗАЩИТЫ НА ОСНОВЕ РАСПОЗНАВАНИЯ ЛИЦ С ПРИМЕНЕНИЕМ МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ОБУЧЕНИЯ СТУДЕНТОВ НАПРАВЛЕНИЯ "ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА"

В статье производится анализ существующих систем биометрической защиты на основе распознавания лиц. Приведены задачи систем данного типа, связанные с биометрическим образом, классификация систем данного типа, методы анализа изображения для поиска лиц. Рассмотрены принципы работы систем биометрической защиты на основе распознавания лиц. Подробно описан метод Виолы-Джонса. Применение данного метода в системе аргументировано. На основе проведённого исследования выше описанные задачи и методы позволяют построить нетребовательную к аппаратным средства опытную систему биометрической защиты на основе распознавания лиц с высокой степенью повторяемости. Построенная система позволит студентам на практике познакомиться с наукой компьютерного зрения.

Ключевые слова: *метод Виолы-Джонса, систем биометрической защиты, распознавание лиц.*

Saraykin M. A., Borisov A.

DEVELOPMENT OF THE SYSTEM OF BIOMETRIC PROTECTION ON THE BASIS OF FACIAL

RECOGNITION USING A MOBILE APPLICATION FOR TRAINING OF STUDENTS OF THE "INFORMATICS AND COMPUTER FACILITIES" DIRECTION

In article the analysis of the existing systems of biometric protection on the basis of facial recognition is made. The tasks of systems of this type connected to a biometric image, classification of systems of this type, methods of the analysis of the image for search of persons are provided. The principles of operation of systems of biometric protection on the basis of facial recognition are considered. Explicitly Viola-Johnes method is described. Application of this method in system with deep arguments. On the basis of the conducted research the described tasks and methods are higher allow to construct the experimental system of biometric protection, undemanding to means equipment rooms, on the basis of facial recognition with a high level of recurrence. The constructed system will allow students to get acquainted in practice with science of computer sight.

Keywords: *Viola-Johnes method, sistem biometric protection, facial recognition.*

В учебном процессе у студентов на сегодняшний день нет возможности познакомиться с наукой компьютерного зрения. Однако, в информационной безопасности сегодня оно используется часто. Примером использования данной технологии является аутентификация пользователя с помощью распознавания лица.

Биометрическая аутентификация - аутентификация пользователя, осуществляемая путем предъявления им своего биометрического образа[1].

Распознавание лиц является одним из биометрических механизмов средств высокоточной биометрической аутентификации человека. Однако, система должна решать дополнительные задачи, связанные с биометрическим образом человека.

Биометрический образ — это образ человека, полученный с выходов первичных измерительных преобразователей физических величин, подвергающийся далее масштабированию и иной первичной обработке с целью извлечения из него контролируемых биометрических параметров человека1.

Задачи системы, связанные с биометрическим образом:

– Создание и хранение биометрических образов

– Формирование сигнала для триггера, если система обнаружила или не обнаружила биометрический образ «Свой».

– Сохранение отчётности за период активности аппаратно-программного комплекса.

– Системы классифицируются по способу работы делятся на три класса:

– Системы, которые способны сравнивать фотографию человека в паспорте и реальное изображение человека. Для таких систем характерно присутствие человека в процессе распознавания. Поэтому система является полуавтоматической.

– Системы, позволяющие осуществлять контроль доступа путём сравнения лица человека и фотографии из базы данных. Однако, для большей безопасности данные системы являются многоступенчатыми – подтверждение личности происходит после прохождения нескольких этапов верификации – по отпечатку пальца, по голосу, пин-коду.

– Системы, позволяющие производить идентификацию личности по видео. Способны идентифицировать движущиеся в потоке лица, производить поиск биометрических

образов, отслеживание и сравнение с базой данных в реальном времени.

Для анализа изображения на наличие лиц из других известных объектов могут быть использованы следующие методы[2]: метод Виолы Джонса, метод сильного уменьшения изображения для сглаживания помех, метод главных компонент, линейный дискриминант Фишера, методы, основанные на геометрических характеристиках лица.

Сегодня в большинстве проектов для обнаружения предметов на фото и видео применяют метод Виолы Джонса. Пол Виола и Майкл Джонс разработали свой метод распознавания в 2001 году[3]. Обобщенный принцип действия алгоритма Виолы-Джонса показан на рисунке 1.

Обучение студентов распознаванию лиц нужно начинать именно с метода Виолы Джонса, т.к. он имеет несколько неоспоримых преимуществ перед другими методами:

– возможность обнаружения нескольких лиц (возможно обнаружение других объектов) на изображении;

– использование несложных классификаторов делает возможным использование этого метода при анализе видеопотока благодаря высокой скорости работы.

Для реализации проекта и добавления возможности расширения функциональности, размещение основной программы будет использован микрокомпьютер Raspberry Pi. В отличие от ПК на данной плате есть выходы GPIO с помощью которых легко можно подключать дополнительные датчики или модули СКУД для дальнейшей модернизации.

Мобильное приложение позволяет дистанционно добавлять участников системы вместе с их биометрическим образом. Дополнительно мобильное приложение способно показывать историю работы системы. Особенностью мобильного приложения станет доступ к базе данных даже при отсутствии интернета (путь прокладывается по наиболее короткому или возможному пути).

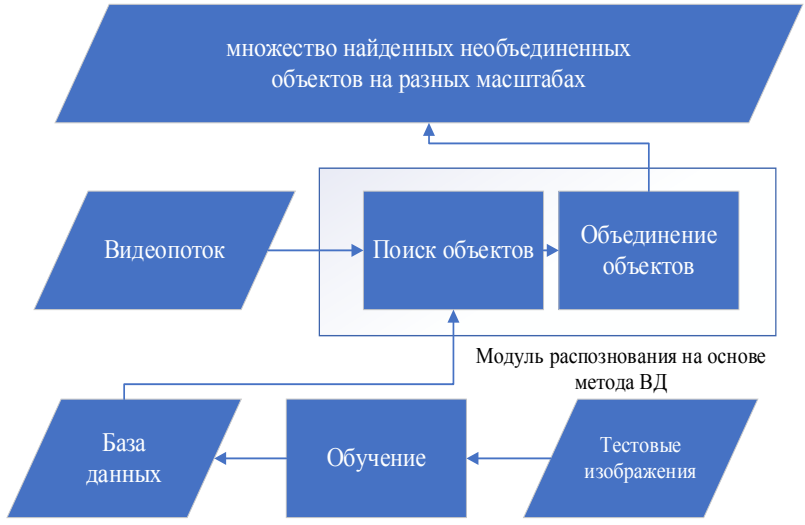

Рисунок 1 - Обобщенный принцип действия алгоритма Виолы-Джонса

Выше описанные задачи и методы позволяют построить нетребовательную к аппаратным средства опытную систему биометрической защиты на основе распознавания лиц с высокой степенью повторяемости.

Литература

1. ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.

2. Моисеевич М.Л. Математические методы распознавания образов». Москва: МГУ, 2004. 42-44 с.

3. Jones P.V.A.M.J. Rapid Object Detection using a Boosted Cascade of Simple Features 2001.

References

1. GOST R 52633.0-2006 Zashchita informatsii. Tekhnika zashchity informatsii. Trebovaniya k sredstvam vysokonadezhnoy biometricheskoy autentifikatsii.

2. Moiseyevich M.L. Matematicheskiye metody raspoznavaniya obrazov». Moskva: MGU, 2004. 42-44 s.

3. Jones P.V.A.M.J. Rapid Object Detection using a Boosted Cascade of Simple Features 2001.

САРАЙКИН Михаил Александрович, студент Алтайского государственного университета имени Ползунова, 656049, Алтайский край, Барнаул, проспект Ленина, 46. E-mail:saraykin1996@gmail.com

БОРИСОВ Алексей Павлович, кандидат технических наук, доцент кафедры «Информатика, вычислительная техника и информационная безопасность» Алтайского государственного технического университета, 656049, г. Барнаул. ул.Ленина, д.46. E-mail: boralp@mail.ru

SARAYKIN Mikhail, student of the Altai state university of Polzunov, 656049, Russia, Altai Krai, Barnaul, Lenin Avenue, 46. E-mail:saraykin1996@gmail.com

BORISOV Aleksey, candidate of technical sciences, associate professor in Altai State Technical University Bld. 656049, Russia, Altai Krai, Barnaul, Lenin Avenue, 46. E-mail: boralp@mail.ru

УДК 004.056.5 + 621.397.01:004.056.5 Вестник УрФО № 4(26) / 2017, с. 9–11

Борисов А. П., Эрнст М. Е.

РАЗРАБОТКА СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ НА ОСНОВЕ RASPBERRY PI ДЛЯ ОБУЧЕНИЯ СТУДЕНТОВ НАПРАВЛЕНИЯ «ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА»

Данная статья посвящена разработке системы видеонаблюдения для обучения студентов направления «Информатика и вычислительная техника». Применительно к практико-ориентированному подходу в современном образовании были сформулированы требования к лабораторной установке. С учетом этих требований была выбрана аппаратная платформа Raspberry Pi и собран прототип устройства.

Ключевые слова: *видеонаблюдение, лабораторная установка, системы технической защиты информации.*

Borisov A. P., Ernst M. E.

DEVELOPMENT OF A VIDEO SURVEILLANCE SYSTEM BASED ON RASPBERRY PI FOR TRAINING STUDENTS DOING A DEGREE IN "INFORMATICS AND COMPUTER SCIENCE"

The article is devoted to the development of video surveillance systems for training students in the field of "Informatics and Computer Science". Taking into account the practice-oriented approach in modern education, there were formulated the requirements for the laboratory unit. Considering these requirements single-board computer Raspberry Pi has been chosen as a hardware platform and there has been created a prototype of the device.

Keywords: *video surveillance, laboratory unit, systems of technical information protection.*

В современных социо-культурных условиях, где ценность информации возрастает экспоненциально, а технологии ее создания, обработки и передачи непрерывно развиваются, становится очевидной необходимость расширения диапазона средств защиты, а так же подготовки высококвалифицированных кадров в области информационных технологий в целом, и информационной безопасности в частности. Необходимым критерием для этого является наличие практических занятий для закрепления теоретических знаний студента.

В учебном плане для специальности «Информатика и вычислительная техника» Алтайского государственно технического университета им.И.И. Полузнова в 2016 году появился курс «Техническое обеспечение систем обработки и защиты информации», который имеет практическую направленность и предполагает получение студентами базовых знаний по работе с различного рода система технической защиты.

Определение «система технической защиты» в данном случае следует рассматривать как комплекс электронных и электрических систем, повышающих безопасность объекта. Данные системы, как правило, являются вспомогательными и позволяют оптимизировать расходы, а также минимизировать влияние «человеческого» фактора. Зачастую они устанавливаются в пределах контролируемой зоны, где размещаются средства криптографической защиты информации.

К системам технической защиты относят и системы контроля и управления доступом (СКУД). Состав их может быть различен, однако в большинстве случаев подсистема видеонаблюдения является одним из неотъемных элементов. Данное направление динамично развивается, и камеры наблюдения встречаются повсеместно, как в составе СКУД, так и как самостоятельные системы безопасности.

Принимая во внимание все эти факторы, можно сделать вывод, что студенты при изучении дисциплины «Техническое обеспечение систем обработки и защиты информации» должны приобрести навыки работы с камерами видеонаблюдения. Для организации эффективного учебного процесса необходимо обеспечить лабораторию соответствующим оборудованием. Исходя из того, что оборудование будет использоваться в учебных целях, необходимо обеспечить его соответствие следующим требованиям: разумное соотношение цена/качество; возможность замены отдельных элементов; модульная структура; простота эксплуатации и ремонта[1].

Приобретение готового продукта не является рациональным решением, так как большинство готовых решений не соответствуют этим требованиям. Таким образом, возникает необходимость создания специализированной камеры видеонаблюдения для использования в учебных целях.[2]

Первым этапом разработки стало создание модели устройства, которая приведена рисунке 1. Данный проект предполагает создание поворотной камеры с аналогом датчика движения и передачей данных непосредственно пользователю, в случае появления объекта на обозначенном расстоянии.

Рисунок 1- Модель устройства

Следующим этапом стал выбор аппаратной составляющей устройства. Были рассмотрены несколько вариантов одноплатных компьютеров, в том числе Raspberry Pi, Orange Pi PC, Intel Galileo, а так же платы на основе микроконтроллеров Arduino. Каждое из приведенных решений имеет свои преимущества, однако в итоге в качестве блока управления был одноплатный компьютер Raspberry Pi Model B, так как на его основе можно относительно просто организовать работу камеры, а также передачу данных конечному пользователю.

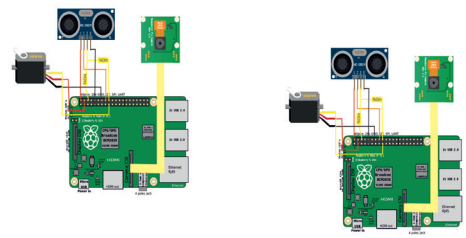

Рисунок 2-Схема подключения элементов к Raspberry Pi

В первую очередь необходимо собрать модуль камеры, который состоит из следующих элементов: дальномер HC-SR04, Привод

SG90, камера Raspberry Pi Zero. На рисунке 2 приведена схема подключения элементов к блоку управления.

Принцип работы модуля заключается в следующем: сервопривод поворачивает установку на угол, заданный пользователем, затем дальномер определяет расстояние до ближайшего объекта и, если это расстояние меньше заданного, камера делает снимок.

На следующем этапе необходимо определиться технологий передачи данных, которая будет использоваться для обеспечения связи с пользователем. Для этого можно использовать уже имеющийся порт LAN. Однако, с целью обеспечения автономности и мобильности устройства, логично использовать беспроводные технологии передачи данных, в данном случае, Wi-Fi.

Для обеспечения обратной связи с пользователем используется мобильное приложение, позволяющее получить изображение с камеры.

Таким образом, создаваемый лабораторный стенд позволит студентам ознакомиться с принципами работы систем видеонаблюдения, технологиями передачи данных, а также применить теоретические знания на практике. Данное устройство может быть легко отремонтировано в случае выхода и строя. Оно так же модифицировано, что расширяет его функционал и, соответственно сферу применения.

Литература

1. Эрнст М.Е., Борисов А.П.Разработка лабораторной установки для студентов направления «Информатики и вычислительная техника»//Использование цифровых средств обучения и робототехники в общем и профессиональном образовании: опыт, проблемы, перспективы. Сборник научных статей III Международной научно-практической конференции— Барнаул 2017. – с. 188–190.

2. См., подр.: Эрнст М.Е., Борисов А.П. К вопросу об использовании систем видеонаблюдения при обучении студентов направления «Информатика и вычислительная техника» // Новая наука: техника и технологии: Международное научное периодическое издание по итогам Международной научно – практической конференции (Уфа, 17 апреля 2017). - Стерлитамак: АМИ, 2017. – №4 - 1. – с.150–152

References

1. Ernst M.Ye., Borisov A.P.Razrabotka laboratornoy ustanovki dlya studentov napravleniya «Informatiki i vychislitel'naya tekhnika»//Ispol'zovaniye tsifrovykh sredstv obucheniya i robototekhniki v obshchem i professional'nom obrazovanii: opyt, problemy, perspektivy. Sbornik nauchnykh statey III Mezhdunarodnoy nauchno-prakticheskoy konferentsii— Barnaul 2017. – s. 188–190.

2. Sm., podr.: Ernst M.Ye., Borisov A.P. K voprosu ob ispol'zovanii sistem videonablyudeniya pri obuchenii studentov napravleniya «Informatika i vychislitel'naya tekhnika» // Novaya nauka: tekhnika i tekhnologii: Mezhdunarodnoye nauchnoye periodicheskoye izdaniye po itogam Mezhdunarodnoy nauchno – prakticheskoy konferentsii (Ufa, 17 aprelya 2017). - Sterlitamak: AMI, 2017. – №4 - 1. – s.150–152

БОРИСОВ Алексей Павлович, кандидат технических наук, доцент кафедры «Информатика, вычислительная техника и информационная безопасность» Алтайского государственного технического университета, 656049, г. Барнаул. ул. Ленина, д.46. E-mail: boralp@mail.ru

ЭРНСТ Марина Евгеньевна, студент Алтайского государственного технического университета, 656049, г. Барнаул. ул. Ленина, д.46. E-mail: ernstmargo@mail.ru

BORISOV Alexey, candidate of technical sciences, associate professor in Altai State Technical University Bld. 46, Lenina Str.,Barnaul, 656049. E-mail: boralp@mail.ru

ERNST Marina, student of Altai State Technical University Bld. 46, Lenina Str.,Barnaul, 656049. E-mail: ernstmargo@mail.ru

УДК 004.056.5 + 005.92:004.63.056 Вестник УрФО № 4(26) / 2017, с. 12–15

Басыров Р. Р., Паршин К. А.

АНАЛИЗ ВЗАИМОСВЯЗИ УГРОЗ И УЯЗВИМОСТЕЙ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

В статье проводится анализ взаимосвязи уязвимостей и угроз информационной безопасности в современных информационных системах электронного документооборота. Рассматриваются основные специфичные процессы обработки информации в системах электронного документооборота. Определены зависимости между процессами по обработке информации, влияющие на защищенность информации в системах ЭДО. На основании проведенных исследований разработана математическая модель вероятности реализации угроз информационной безопасности в зависимости от вероятности реализации той или иной уязвимости. Дана оценка защищенности современных систем ЭДО.

Ключевые слова: *документ, информация, информационная безопасность, угроза, уязвимость, документооборот, реквизит, защита информации, система электронного документооборота.*

Basyirov R. R., Parshin K. A.

ANALYSIS OF THE RELATIONSHIP BETWEEN THREATS AND VULNERABILITIES IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

The article analyzes the correlation of vulnerabilities and threats to information security in modern information systems of electronic document management. The main specific processes of information processing in electronic document management systems are considered. Dependencies between information processing processes affecting the security of information in EDM systems have been determined. Based on the conducted research, a mathematical model of the probability of implementing information security threats has been developed, depending

on the likelihood of the implementation of a particular vulnerability. The evaluation of the security of modern EDM systems is given.

Keywords: *document, information, information security, threat, vulnerability, document circulation, props, information protection, electronic document management system.*

В связи с бурным информационным развитием общества и производства, в большинстве государственных, муниципальных учреждений, а также многих крупных коммерческих организациях внедряются системы электронного документооборота. Данные системы позволяют разгрузить бюрократическую машину в организации, повысить темпы работы по обработке информации содержащейся в документах, предоставить мобильный доступ к документам, повысить трудовую дисциплину сотрудников за счет автоматизированных средств контроля работы с документами.

Однако при всех положительных результатах использования систем электронного документооборота, возникают угрозы информационной безопасности, присущие всем автоматизированным информационным системам. Таким образом, определение взаимосвязи угроз безопасности информации, хранящейся и обрабатываемой в СЭД, позволит создать эффективную методику использования методов и средств защиты информации для достижения необходимого уровня защищенности системы.

Для реализации поставленной задачи, в первую очередь, необходимо определить основные процессы по обработке информации, протекающие в электронном документообороте. Согласно определению, процесс документооборота заключается в движение документов в организации с момента их создания или получения до завершения исполнения или отправки[1]. Таким образом можно выявить основные процессы обработки информации, протекающие в документообороте:

1) создание документа;

2) получение документа;

3) исполнение документа;

4) отправка документа;

Проведя анализ информационных потоков и информации, обрабатываемой в данных процессах, можно выделить следующие информационные группы:

1 – Содержание документа;

2 – Реквизиты документа;

3 – Информация о согласовании документа;

4 – Информация об исполнении документа;

Отметим, что информация, относящаяся к 1 и 2 группе, является обязательной и без неё электронный документ не может существовать. Информация из 3 и 4 группы может отсутствовать в документе, но при её наличии непосредственно характеризует информацию из 1 и 2 группы.

Для информации относящееся любой из этих групп характерны следующие уязвимости, нарушающие состояние защищенности: нарушение конфиденциальности, нарушение целостности, блокирование доступности информации, содержащейся в электронном документе. Введем условное обозначение для таких уязвимостей: V_n^m, где V – уязвимость, нарушающее состояние защищенности информации, относящейся к *n = 1...4* группе, в результате применения *m = к, ц, д* воздействия.

Изучив рынок современны систем электронного документооборота, проведя анализ технологии формирования информационных потоков в таких системах и учитывая взаимосвязь информационных групп, были сделаны выводы о взаимосвязи уязвимостей и угроз, возникающих в результате их реализации. Вероятность возникновения события $P(T_n^m)$, нарушающего состояние защищенности информации, характеризуется вероятностью использования уязвимости и/или совокупности уязвимостей[2,3].

Далее выведены формулы для расчета вероятностей возникновения угроз в СЭД для каждой информационной группы в зависимости от реализованных уязвимостей.

Вероятности угрозы нарушения конфиденциальности информации:

$$P(T_1^к)=P(T_1^к|V_2^ц)*P(V_2^ц)+P(T_1^к|V_3^к)*P(V_3^к)+P(T_1^к|V_4^к)*P(V_4^к) \quad (1)$$

$$P(T_2^к)=P(T_2^к|V_2^ц)*P(V_2^ц)+P(T_2^к|V_3^к)*P(V_3^к)+P(T_2^к|V_4^к)*P(V_4^к) \quad (2)$$

$$P(T_3^к)=P(T_3^к|V_2^ц)*P(V_2^ц)+P(T_3^к|V_3^к)*P(V_3^к) \quad (3)$$

$$P(T_4^к)=P(T_4^к|V_2^ц)*P(V_2^ц)+P(T_4^к|V_4^к)*P(V_4^к) \quad (4)$$

Вероятности угрозы нарушения целостности информации:

$$P(T_1^ц)=P(T_1^ц|V_2^ц)*P(V_2^ц)+P(T_1^ц|V_1^ц)*P(V_1^ц) \quad (5)$$

$$P(T_2^ц)=P(V_2^ц) \quad (6)$$

$$P(T_3^ц)=P(T_3^ц|V_2^ц)*P(V_2^ц)+P(T_3^ц|V_2^ц)*P(V_3^ц) \quad (7)$$

$$P(T_4^ц)=P(T_4^ц|V_2^ц)*P(V_2^ц)+P(T_4^ц|V_2^ц)*P(V_4^ц) \quad (8)$$

Вероятности угрозы нарушения доступности информации:

$$P(T_1^д)=P(T_1^д|V_2^ч)*P(V_2^ч)+P(T_1^д|V_1^ч)*P(V_1^ч) \quad (9)$$

$$P(T_2^д)=P(T_2^д|V_2^ч)*P(V_2^ч)+P(T_2^д|V_2^д)*P(V_2^д) \quad (10)$$

$$P(T_3^д)=P(T_3^д|V_2^ч)*P(V_2^ч)+P(T_2^д|V_3^ч)*P(V_3^ч)+P(T_2^д|V_3^д)*P(V_3^д) \quad (11)$$

$$P(T_4^д)=P(T_4^д|V_2^ч)*P(V_2^ч)+ P(T_2^д|V_4^ч)*P(V_4^ч)+P(T_2^д|V_4^д)*P(V_4^д) \quad (12)$$

Исходя из рассмотренных вероятностей, следует выделить уязвимость нарушения целостности реквизитов документа $P(V_2^ч)$, так как именно реквизиты документа определяют права пользователей на работу с документами. Иными словами, изменяя реквизиты документа, злоумышленник получает возможность управлять движением документа в системе, а соответственно изменять, получать и блокировать доступ, к информации, содержащейся в самом документе, и как следствие, к информации, содержащейся во всех процессах жизненного цикла документа[4,5].

Вероятность использования той или иной уязвимости, в свою очередь, определяется совокупностью следующих технических параметров системы:

1) Вид используемой в системе БД;

2) Способы аутентификации пользователей;

3) Открытость исходного кода;

4) Внутренняя архитектура взаимодействия модулей системы;

5) Наличие и способ реализации WEB-интерфейса;

6) Механизм подписания документа (включая виды используемых ЭП);

7) Наличие механизмов шифрования БД.

8) Протоколирование действий пользователя и системы, а также доступность данных протоколов.

Таким образом, согласно предложенной модели взаимосвязи уязвимостей и угроз безопасности информации в системах электронного документооборота можно установить, что одним из параметров, оказывающих наибольшее влияние на общий уровень защищенности системы электронного документооборота, являются уязвимости связанные с нарушением целостности реквизитов. Эффективными техническими мерами устранения данной угрозы является использование средств, направленных на контроль и управление доступом пользователей к ресурсам системы, а также использование электронной подписи позволяющей контролировать факт достоверности электронного документа.

Литература

1. ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения.

2. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

3. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

4. ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

5. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

References

1. GOST R 7.0.8-2013. Natsional'nyy standart Rossiyskoy Federatsii. Sistema standartov po informatsii, bibliotechnomu i izdatel'skomu delu. Deloproizvodstvo i arkhivnoye delo. Terminy i opredeleniya.

2. GOST R 53114-2008 Zashchita informatsii. Obespecheniye informatsionnoy bezopasnosti v organizatsii. Osnovnyye terminy i opredeleniya».

3. GOST R ISO/MEK 15408-2-2008 Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. Chast' 2. Funktsional'nyye trebovaniya bezopasnosti.

4. GOST R ISO/MEK TO 19791-2008 Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Otsenka bezopasnosti avtomatizirovannykh sistem.

5. GOST R 51275-2006 Zashchita informatsii. Ob"yekt informatizatsii. Faktory, vozdeystvuyushchiye na informatsiyu. Obshchiye polozheniya

БАСЫРОВ Руслан Равильевич, аспирант кафедры «Информационные технологий и защита информации» Уральского государственного университета путей сообщения; 620034, г. Екатеринбург, ул. Колмогорова, 66, RRBasyirov@usurt.ru

ПАРШИН Константин Анатольевич, канд. тех. наук, доцент «Информационные технологий и защита информации» Уральского государственного университета путей сообщения; 620034, г. Екатеринбург, ул. Колмогорова, 66, KParshin@usurt.ru

BASYROV Ruslan Ravilevich, Postgraduate at the Department of «Information technologies and protection of information», Ural State University of Railway Transport, 620034, Ekaterinburg, Kolmogorov street, 66, RRBasyirov@usurt.ru

PARSHIN Konstantin Anatolevich, Candidate of Engineering Sciences, Associate Professor at the Department of «Information technologies and protection of information», Ural State University of Railway Transport, 620034, Ekaterinburg, Kolmogorov street, 66, KParshin@usurt.ru

УДК 004.056.5 + 656.2:004.056.5 Вестник УрФО № 4(26) / 2017, с. 16–20

Паршин К. А., Подгорный М. С.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА ПУТЕМ МОНИТОРИНГА ТЕКСТОВЫХ ПУБЛИКАЦИЙ В ОТКРЫТЫХ ИСТОЧНИКАХ ДАННЫХ

Статья посвящена рассмотрению проблемы распространения информации ограниченного доступа путем публикации текстовых данных в открытых источниках, таких как веб-порталы, интернет-сервисы и социальные сети. Основной предметной областью в статье является сфера железнодорожного транспорта. Рассмотрены методы работы с текстовыми данными, применяемые в системах предотвращения утечек информации, которые могут быть использованы в альтернативных программных продуктах. Акцент сделан на уникальность терминологии, используемой только в железнодорожной отрасли на всей территории Российской Федерации. Определен перечень признаков, характерных только к сокращениям железнодорожных объектов и субъектов.

Ключевые слова: *информационная безопасность, железнодорожный транспорт, мониторинг публикаций, открытые источники данных, методы анализа текстовых данных, терминология железнодорожной отрасли.*

ENSURING INFORMATION SECURITY OF RAILWAY TRANSPORT ENTERPRISE BY MONITORING TEXT PUBLICATIONS IN OPEN DATA SOURCES

The article is devoted to problems of dissemination limited access information by publishing text data in open sources, such as web portals, Internet services and social networks. The main subject area in the article is the sphere of railway transport. The article describes methods of working with text data used in Data leakage prevention systems that can be used in alternative software products. The emphasis of article is on the unique terminology used only in railway industry throughout the Russian Federation. A list of features characteristic only of abbreviations of railway objects and subjects was determined.

Keywords: *information security, railway transport, monitoring of publications, open data sources, methods for analyzing text data, railway industry terminology.*

Сфера железнодорожного транспорта Российской Федерации занимает существенное место в экономике страны. По отчету с официального сайта вклад ОАО «РЖД» составляет 2,5% при среднем обороте денежных средств, практически, в два триллиона рублей. Сеть железных дорог покрывает всю заселенную территорию страны и включает в себя 16 железных дорог. К территории Уральского федерального округа относятся Свердловская и Южно-Уральская железные дороги. Существенным показателем для ОАО «РЖД» является количество сотрудников предприятия – на 2017 год данный показатель достигает 890 тысяч человек[1].

Для любого предприятия с большим количеством сотрудников важным является вопрос обеспечения высокого уровня информационной безопасности для документов и данных, оборачиваемых внутри компании. Особо чувствительным моментом для подобного предприятия является публикация данных, содержащих информацию ограниченного доступа в сети Интернет, так как помимо самого распространения информации, происходит и негативное представление компании в открытой сети, что несет за собой различные экономические и социальные последствия. Примером подобных публикаций может быть случай закрепления на одном из публичных сайтов служебной переписки между поездным и станционным диспетчерами, а также машинистом локомотива после столкновения пассажирского и пригородного поездов на Московской железной дороге[2]. Статья на сайте содержала в себе практически всю текстовую запись разговора между причастными сотрудниками и была удалена лишь через неделю после публикации. Ключевым моментом в записи разговора было то, что в тексте использовались сокращения должностей, которые могут быть использованы только на железнодорожном транспорте (ДС, ДНЦ, ДСП).

Далее в работе рассматриваются методы по поиску текстовых записей на определенных публичных сайтах сети Интернет с целью уменьшения «времени жизни» подобных публикаций, что приведет к снижению негативного эффекта для компании.

Важным программным компонентом в области защиты информации на любом крупном предприятии являются системы предотвращения утечек информации *(Data Leak Prevention, DLP)*. Богатый функционал данных систем (методы работы с текстом, *OCR*, аудио-

и видеоанализ) позволяет определить возможную подобную запись еще на уровне закрепления текста публикации на том или ином форуме или профиле в социальной сети. Однако по большей части весь поиск и предотвращение возможны лишь в зоне действия внутренней сети предприятия (рис. 1). Статья может быть закреплена и со своего личного персонального компьютера или мобильного устройства через любую другую точку доступа. Именно поэтому, а также ввиду экономических ситуаций, предприятию требуются альтернативные методы и программные средства для поиска данных записей.

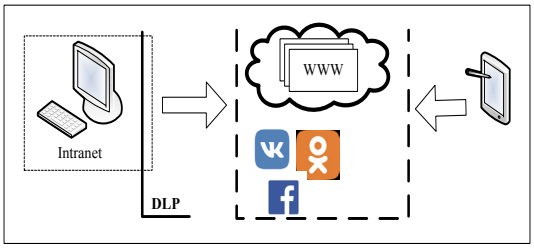

Рис. 1. Условная схема возможных публикаций

Однако стоит обратить внимание на программно-аналитические методы, которые используются в системах предотвращения утечек информации для работы с текстовыми данными:

– поиск по регулярным выражениям;

– предустановленные текстовые шаблоны;

– предустановленные тематические словари.

Именно на данных методах сделан упор в текущей работе ввиду особенности описания объектов и субъектов на железнодорожном транспорте. В отличие от систем предотвращения утечек информации местом поиска и анализа данных является не источник информации, а именно получатель информации, то есть заранее определенный пополняемый перечень веб-сайтов, интернет-сервисов, а также профилей пользователей и групп в социальных сетях. Целью мониторинга является именно уменьшение времени нахождения публикации в открытом доступе.

Как уже говорилось ранее, в сфере железнодорожного транспорта существует определенная терминология для описания тех или иных объектов или субъектов, единая на всей территории страны. Например, для описания должности поездного диспетчера используется сокращенное наименование ДНЦ. Термин не является какой-либо расшифровкой и имеет свои исторические корни[3].

Аналогичные сокращения имеют и объекты инфраструктуры на железнодорожном транспорте, например ДЦС или ВЧД. Уникальностью описания обладают и данные передаваемые в информационных системах. Любой документ, передаваемый по внутренним каналам связи, содержит как минимум телеграфный код причастных дирекций или служб, а также шифр исполнителя данного документа. Все это говорит о том, что предметная область в части железнодорожной терминологии заслуживает большого внимания при работе с текстовыми данными.

Регулярные выражения могут быть использованы при поиске и анализе следующих специфических элементов в общем тексте:

– телеграмма натурный лист грузового поезда (ТГНЛ) – уникальный цифровой код, описывающий содержание вагонов в грузовом поезде[4];

– сообщения системы АСОУП[5] – цифровой код, содержащий уникальные комбинации цифр и знаков пунктуации.

Кроме информационных систем, уникальностью и синтаксическими особенностями обладают и сами термины. Первой отличительной чертой железнодорожной терминологии является то, что объекты имеют определенную условную иерархичность (рис. 2).

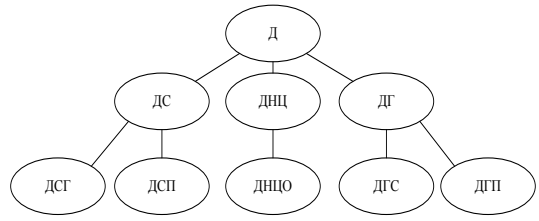

Рис. 2. Иерархичность в описании субъектов службы перевозок

Вторым признаком является условное наследование. Например, следующее описание должностей Службы перевозок:

– Д – Служба перевозок;

– ДС – начальник станции;

– ДСП – дежурный по станции;

– ДСПГ – дежурный по сортировочной горке;

– ДСПГО – оператор при дежурном по сортировочной горке.

Третьей особенностью является именно синтаксический состав и порядок букв в со-

кращении железнодорожных объектов и субъектов. При анализе выборки терминов[6], состоящей из 500-600 сокращений, была получена следующая статистика:

– общее количество символов в выборке равно 1583;

– общее количество согласных букв в выборке 81,81 %;

– количество терминов, начинающихся с гласной буквы 19,47 %;

– количество терминов, заканчивающихся гласной буквой 15,97 %.

Другими словами при текстовом анализе данных важно обращать внимание именно на наполнение и расположение в словах (токенах) согласных букв. Ниже представлена гистограмма (рис. 3) частоты встречи шаблонных терминов, содержащих согласные и гласные буквы («С» и «Г» соответственно).

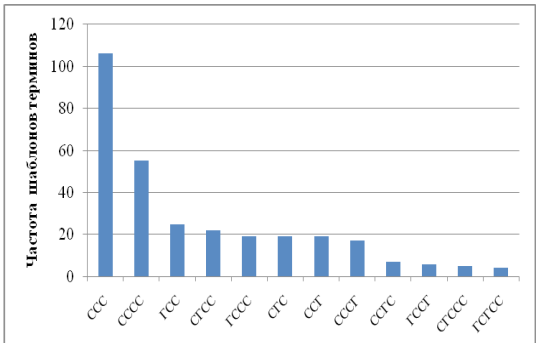

Рис. 3. Частотные показатели шаблонов терминов

Из графика видно, что наибольшей частотой обладают термины, состоящие из трех и четырех согласных букв («ССС» и «СССС» соответственно).

Из вышеописанных характеристик можно сделать вывод, что для поиска железнодорожных терминов могут быть использованы как заранее подготовленные словари, так и определенные подготовленные шаблоны.

При формировании тезауруса могут быть использованы следующие источники данных:

– специализированная железнодорожная литература;

– нормативные и правовые документы компании, а также дочерних и зависимых обществ;

– информационные системы;

– иные источники информации.

Синтаксические характеристики могут быть использованы при формировании заранее подготовленных текстовых шаблонов или «масок» поиска, аналогичных регулярным выражениям, но являющихся более гибкими при настройке. При работе с данными шаблонами важным моментом может быть ложное срабатывание в процессе определения термина, так как сокращение может относиться к сфере строительства, авиаперевозок или другой подобной сфере деятельности. Другими словами, в результате может быть получена неверная классификация термина.

Подведя итоги можно сказать, что уникальность терминологии железнодорожного транспорта содержит в себе большое количество признаков, которые могут быть использованы при мониторинге текстовых записей в сети интернет с использованием методов анализа текстовых данных. В дальнейших исследованиях планируется более подробно раскрыть тематику применения терминологии железнодорожного транспорта и через программные компоненты выполнить контрольные проверки методов при получении данных с профилей пользователей социальных сетей.

Литература

1. Показатели основной деятельности [Электронный ресурс] // официальный сайт, 2017. URL: http://ir.rzd.ru/static/public/ru?STRUCTURE_ID=63 (дата обращения: 10.11.2017).

2. Про столкновение электрички и поезда [Электронный ресурс] // форум, 2017. URL: http://www.yaplakal.com/forum15/st/175/topic1579951.html (дата обращения: 12.04.2017).

3. Общий курс железных дорог: Учебник для техникумов и колледжей ж.-д. транспорта / В.Н. Соколов, В.Ф. Жуковский, С.В. Котенкова, А.С. Наумов; Под редакцией В.Н. Соколова. — М.: УМК МПС России, 2002. С. 180—200.

4. Телеграмма-натурный лист поезда (ТГНЛ) [Текст] : методические указания / [С. А. Бессоненко и др.] ; Сибирский гос. ун-т путей сообщения (СГУПС).—2-е изд., измененное и доп. — Новосибирск: СГУПС, 2015. С. 30.

5. Санькова Г.В. Информационные технологии в перевозочном процессе: учебное пособие / Г.В. Санькова, Т.А. Одуденко. — Хабаровск: Изд-во ДВГУПС, 2012. — С. 64.

6. Железнодорожный словарь [Электронный ресурс] // форум, 2017. URL: http://rzd.me/inform-block/zhd-slovar/ (дата обращения: 20.10.2017).

References

1. Pokazateli osnovnoj deyatelnosti [Elektronnyy resurs] // oficialnyj sajt, 2017. URL: http://ir.rzd.ru/static/public/ru?STRUCTURE_ID=63 (data obrashcheniya: 10.11.2017).

2. Pro stolknovenie ehlektrichki i poezda [Elektronnyy resurs] // forum, 2017. URL: http://www.yaplakal.com/forum15/st/175/topic1579951.html (data obrashcheniya: 12.04.2017).

3. Obshchij kurs zheleznyh dorog: Uchebnik dlya tekhnikumov i kolledzhej zh.-d. transporta / V.N. Sokolov, V.F. ZHukovskij, S.V. Kotenkova, A.S. Naumov; Pod redakciej V.N. Sokolova. — M.: UMK MPS Rossii, 2002. S. 180—200.

4. Telegramma-naturnyy list poezda (TGNL) [Tekst] : metodicheskie ukazaniya / [S. A. Bessonenko i dr.] ; Sibirskyy gos. un-t putej soobshcheniya (SGUPS).—2-e izd., izmenennoe i dop. — Novosibirsk: SGUPS, 2015. S. 30.

5. Sankova G.V. Informacionnye tekhnologii v perevozochnom processe: uchebnoe posobie / G.V. Sankova, T.A. Odudenko. — Habarovsk: Izd-vo DVGUPS, 2012. — S. 64.

6. ZHeleznodorozhnyy slovar [Elektronyy resurs] // forum, 2017. URL: http://rzd.me/inform-block/zhd-slovar/ (data obrashcheniya: 20.10.2017).

ПАРШИН Константин Анатольевич, кандидат технических наук, доцент кафедры «Информационные технологии и защита информации», Уральский государственный университет путей сообщения, 620034, Свердловская обл., г. Екатеринбург, ул. Колмогорова, 66. E-mail: kparshin@usurt.ru

ПОДГОРНЫЙ Михаил Сергеевич, аспирант кафедры «Информационные технологии и защита информации», Уральский государственный университет путей сообщения, 620034, Свердловская обл., г. Екатеринбург, ул. Колмогорова, 66. E-mail: podgorny312@yandex.ru

PARSHIN Konstantin, PhD, associate professor of «Information technologies and information security», Ural State University of Railway Transport, 620034, Sverdlovsk region, Yekaterinburg, Kolmogorova St., 66. E-mail: kparshin@usurt.ru

PODGORNYY Mihail, graduate student of «Information technologies and information security», Ural State University of Railway Transport, 620034, Sverdlovsk region, Yekaterinburg, Kolmogorova St., 66. E-mail: podgorny312@yandex.ru

УДК 004:338 + 004.738.5:336.743 Вестник УрФО № 4(26) / 2017, с. 21–24

Осипов Н. Р., Кротова Е. Л.

БЛОКЧЕЙН – ПЛАТФОРМА ДЛЯ ИННОВАЦИЙ

В настоящее время жизнь человека связана с новыми технологиями, информацией, деньгами и многочисленными бумагами. Для достижения тех или иных задач приходится привлекать многочисленных посредников, сотрудничество с которыми подразумевает проведение десятков разных операций. Также это накладывает временные и материальные ограничения в виде комиссии посредников и бумажной проволочки. Задача технологии блокчейн — исправить проблему, которая связана со значительными материальными (оплачиваемые посреднические услуги) и временными затратами.

Ключевые слова: *Блокчейн, криптовалюта, цепочки блоков транзакций, биткоин.*

Osipov N. R., Krotova E .L.

BLOCKCHAIN – A PLATFORM FOR INNOVATION

At the now day, a person's life is connected with new technologies, information, money and numerous papers. To perform different tasks, it is necessary to involve numerous intermediaries, cooperation with which implies performing different operations. It also imposes temporary and material restrictions in the form of a commission of intermediaries and "paper" delay. The task of blocking technology is to fix a problem that is associated with significant material (paid intermediary services) and time costs.

Keywords: *Blocking, crypto currency, chain of transaction blocks, bitcoin.*

Что такое блокчейн и его актуальность

Блокчейн означает «цепь блоков». Блоком называют такой информационный пакет, содержащий в себе все предыдущие сведения и часть новых. А вся цепочка представляет собой распределенную между множеством участников базу данных, работающую без централизованного управления.

Отсутствие централизации - важный элемент технологии. Все сведения хранятся на компьютерах пользователей, которые видят одно и то же. Поэтому взломать или «выключить» блокчейн невозможно: если есть хотя бы один компьютер, включенный в сеть, технология будет работать.

Кроме того, система организована так, что каждый ее участник постоянно проверяет поступающие к нему сведения. В итоге при любой операции подтверждается целостность и достоверность хранящихся в сети материалов.

Новая информация записывается в конец цепочки поверх уже проверенной и частично основывается на ней. Если изменить какую-то

часть материалов, например, путем взлома, то это должно привести к изменению последующей цепочки информации, иначе эта ошибка будет видна всем участникам. А изменить данные сразу, например, на десяти тысячах компьютеров очень сложно и дорого. Этим гарантируется сохранность и точность сведений.

Сегодня мы уже все привыкли делиться информацией через децентрализованную интерактивную платформу Интернета. Но когда речь заходит о пересылке ценностей (денег), мы обычно вынуждены снова пользоваться услугами старых централизованных финансовых учреждений (банков). Да, методы платежей через Интернет появились сразу же в момент рождения этой сети (наиболее очевидный пример — это PayPal), но они, как правило, требуют интеграции с банковским счетом или кредитной картой, иначе их нельзя реально использовать.

Технология блокчейн предлагает заманчивую возможность избавиться от этого «лишнего звена». Она может взять на себя все три важные роли, которые традиционно играет сектор финансовых услуг: регистрация сделок, подтверждение подлинности личности и заключение контрактов.

Это будет иметь огромное значение, поскольку во всем мире рынок финансовых услуг — самый большой по рыночной капитализации. Перевод хотя бы части этой системы на технологию блокчейн приведет к разрыву большого числа связей в сфере финансовых услуг, но одновременно позволит значительно повысить эффективность этих услуг.

Возможности этой технологии в заключении контрактов могут оказаться очень полезными и вне сектора финансовых услуг. Помимо ввода в обращение еще одной валюты (биткоина), технология блокчейн может использоваться также для хранения любого вида цифровой информации, включая компьютерный код.

Этот фрагмент кода можно запрограммировать так, чтобы он выполнялся, только когда обе договаривающиеся стороны вводят свои ключи, тем самым соглашаясь на заключение контракта. Этот же код может получать информацию из внешних потоков данных (цены на акции, метеорологические сводки, заголовки новостей и все остальное, что может быть проанализировано компьютером) и составлять контракты, которые будут *автоматически* регистрироваться при выполнении определенных условий.

Этот механизм называется «умные контракты», и возможности их применения практически бесконечны.

Например, интеллектуальная система терморегуляции может передавать данные об энергопотреблении в интеллектуальную электрическую сеть. При потреблении определенного количества электроэнергии другая цепочка блоков автоматически переводит нужную сумму с вашего счета на счет энергетической компании. В результате автоматизируются работа счетчика и процесс выставления счетов.

Можно также использовать этот подход для контроля использования интеллектуальной собственности, определяя, сколько раз пользователь может получить доступ к информации, поделиться ею или скопировать ее. Еще его можно использовать для создания систем голосования с защитой от фальсификаций, распространения информации без цензурных ограничений и многого другого.

Принцип работы

Иногда технологию блокчейн называют «Интернетом ценностей», и мы считаем, что это хорошая метафора.

Каждый человек может разместить в Интернете информацию, а затем другие люди могут получить к ней доступ из любой точки мира. Цепочки блоков позволяют отправлять в любую точку мира, где будет доступен файл блокчейна, какие-либо ценности. Но у вас должен быть закрытый ключ, созданный по криптографическому алгоритму, чтобы разрешить вам доступ только к тем блокам, которыми вы «владеете».

Предоставляя кому-либо ваш закрытый ключ, вы, по сути, передаете этому лицу денежную сумму, которая хранится в соответствующем разделе цепочки блоков.

В случае биткоинов такие ключи используются для доступа к адресам, по которым хранятся некоторые суммы в валюте, представляющие прямую финансовую ценность. Этим реализуется функция регистрации перевода средств, обычно такую роль выполняют банки.

Кроме того, реализуется еще одна важная функция: установка отношений доверия и подтверждение подлинности личности, потому что никто не может изменять цепочку блоков без соответствующих ключей. Изменения, не подтвержденные этими ключами, отклоняются. Конечно, ключи (как и физическая валюта) теоретически могут быть украдены, но

защита нескольких строк компьютерного кода обычно не требует больших затрат.

Это означает, что основные функции, выполняемые банками: проверка подлинности личности (для предотвращения мошенничества) и последующая регистрация сделок (после чего они становятся законными) — могут выполняться цепочкой блоков быстрее и точнее[1].

Итак, из чего же состоит технология блокчейн?

1. Участники

Все участники системы делятся на 2 категории:

– рядовые пользователи, создающие записи (операции, действия, транзакции);

– майнеры, которые формируют из них блоки (пакеты, конверты) данных. Это очень сложная и ресурсоемкая процедура, и не каждый участник имеет техническую возможность ее реализации.

Обычный пользователь записывает в систему сообщение, например, о том, что «X взял кредит у Y». Оно зашифровано. Причем X и Y имеют свои ключи[2].

Каждый участник, получив эти сведения, проверяет шифры и распространяет сообщение по сети. Если в шифровке обнаружена ошибка, данные остальным пользователям не отправляются.

2. Формирование блоков

Майнеры, получив записи, проверяют их, пакуют в блоки и также рассылают по сети. Пока данные не запакованы, они считаются недостоверными.

Блок состоит из 2 частей: тела и заголовка. Тело — это набор записанных сообщений. Заголовок — связующее звено цепи. Он содержит 2 ключа:

– предыдущего набора материалов;

– и текущего блока, который рассчитан на основе содержащихся в нем записей, и шифра предшествующего конверта.

Таким образом, в каждом запакованном наборе материалов закодирована вся предыдущая информация. Любое изменение сведений потребует корректировки ключа текущего пакета и всех последующих. Другими словами, видя систему и зная коды, можно понять, не нарушен ли порядок конвертов, не удалены или не добавлены ли новые наборы, соответствуют ли сведения шифровке и т. п.

4. Формирование ключей

Ключи получаются путем хэширования или свертки — преобразования информации в число. Проиллюстрируем простым примером. Вместе со словом «деньги» передается его код, представляющий собой произведение чисел - порядковых номеров букв, из которых состоит слово «деньги». Получатель слова перемножает номера букв и сверяется с кодом. Так происходит проверка. Если в процессе передачи «деньги» трансформировались в «денги», то получатель, увидев несоответствие между полученным кодом и рассчитанным им самим результатом поймет, что данные искажены.

Это самый простой пример, приведенный для наглядности. Более сложную защиту в блокчейн дает криптографическое шифрование, которое применяется в электронной подписи. В итоге код может представлять собой число, состоящее из нескольких десятков цифр.

Кроме того, для повышения безопасности, создатели сетей блокчейн разрабатывают дополнительные условия кодировки. Так, в сети биткоин, каждый ключ начинается с десяти нулей. Поэтому майнеры должны проводить сотни и миллионы вычислений для соответствия требованиям формирования кода.

5. Зашифровка записей

Записи также объединены в цепочки. Никто не может создать злонамеренное сообщение «перечислить все средства Y на счет X, открытый в оффшорном банке», так как все операции содержат в себе ссылку на предшествующее сообщение (источник).

Запись имеет 2 части: источник и результат. Источник включает в себя шифр предыдущей операции и разблокирующее правило. Результат — содержание текущей операции и блокирующее условие. Создать следующее сообщение и продлить цепь записей сможет только тот, кому известно разблокирующее правило.

Например, предыдущая операция (источник) имела результат «перевести компании X сумму, равную 1000 денег». Блокирующее условие было таким: «код пароля — 56739209871...». Для того чтобы получить и потратить эту сумму, компания X должна создать следующее сообщение, включив в ее разблокирующее правило этот пароль. А само это правило будет гласить «Рассчитать ключ пароля NNNN». Майнер, получив запись, подставляет результат расчета в предыдущее сообщение цепочки, и если все сходится, включает ее в пакет[3].

Заключение

Таким образом, технология блокчейн делает возможным хранение данных о финансовых операциях, юридических обязательствах, правах собственности, обеспечивая полную прозрачность и всеобщую доступность для ознакомления, но при этом надежно защищая от любого подлога, взлома и так далее. В еще более простом варианте можно сказать, что технология блокчейн — это некий стеклянный куб с постоянно включенной камерой наблюдения — в него можно (под присмотром) положить что-то новое, но при попытке изменения или подмены содержимого это тут же станет видно любому наблюдателю.

Также он может применяться не только в описанных сферах, но и в страховании, налогообложении, риэлтерских услугах, сделках с имуществом, логистике, избирательной системе и других сферах, что делает эту технологию платформой для дальнейших инноваций.

Литература

1. Что такое Блокчейн? // 24PAYBANK. URL: https://24paybank.com/faq/chto-takoe-blockchain.html (дата обращения 10.06.2017)

2. Блокчейн - это… Как работает блокчейн, преимущества, применение, перспективы. // fb.ru URL: http://fb.ru/article/261672/blokcheyn---eto-kak-rabotaet-blokcheyn-preimuschestva-primenenie-perspektivyi (дата обращения 11.06.2017)

3. Технология Блокчейн (blockchain) – что это такое простыми словами. // real-investment.ru URL: http://real-investment.ru/finansovaja_gramotnost/blokchejn_blockchain_chto_ehto_takoe_prostymi_slovami (дата обращения 15.06.2017)

4. Что такое блокчейн? Расскажем простыми словами. // Coinspot URL: https://coinspot.io/beginners/chto-takoe-blokchejn-rasskazhem-prostymi-slovami/ (дата обращения 17.06.2017)

5. Что такое блокчейн и зачем он нужен // Хабрахабр URL: https://habrahabr.ru/company/bitfury/blog/321474/ (дата обращения 20.06.2017)

References

1. Chto takoye Blokcheyn? // 24PAYBANK. URL: https://24paybank.com/faq/chto-takoe-blockchain.html (data obrashcheniya 10.06.2017).

2. Blokcheyn - eto… Kak rabotayet blokcheyn, preimushchestva, primeneniye, perspektivy. // fb.ru URL: http://fb.ru/article/261672/blokcheyn---eto-kak-rabotaet-blokcheyn-preimuschestva-primenenie-perspektivyi (data obrashcheniya 11.06.2017).

3. Tekhnologiya Blokcheyn (blockchain) – chto eto takoye prostymi slovami. // real-investment.ru URL: http://real-investment.ru/finansovaja_gramotnost/blokchejn_blockchain_chto_ehto_takoe_prostymi_slovami (data obrashcheniya 15.06.2017).

4. Chto takoye blokcheyn? Rasskazhem prostymi slovami. // Coinspot URL: https://coinspot.io/beginners/chto-takoe-blokchejn-rasskazhem-prostymi-slovami/ (data obrashcheniya 17.06.2017).

5. Chto takoye blokcheyn i zachem on nuzhen // Khabrakhabr URL: https://habrahabr.ru/company/bitfury/blog/321474/ (data obrashcheniya 20.06.2017).

ОСИПОВ Никита Романович, студент кафедры Автоматики и телемеханики Пермского национального исследовательского политехнического университета. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: nikita.osipov.96@yandex.ru

КРОТОВА Елена Львовна, кандидат физико-математических наук, кафедра Высшей математики Пермского национального исследовательского политехнического университета, доцент. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

OSIPOV Nikita, student of the Department of Automation and Telemechanics of the Perm National Research Polytechnic University. 29 Komsomolsky prospekt, Perm, Perm krai, Russia, 614990. E-mail: nikita.osipov.96@yandex.ru

KROTOVA Elena, candidate of physico-mathematical sciences, Department of Higher mathematics, Perm National Research Polytechnic University, docent. 29 Komsomolsky prospekt, Perm, Perm krai, Russia, 614990. E-mail: lenkakrotova@yandex.ru

УДК 003.26 + 004.056.55 Вестник УрФО № 4(26) / 2017, с. 25–27

Филиппов М. А., Кротова Е. Л.

КВАНТОВАЯ КРИПТОГРАФИЯ. ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

Статья посвящена квантовой криптографии, её отличиям от традиционной криптографии. Особое внимание авторы уделяют преимуществам и недостаткам квантовой криптографии и её актуальности в современном мире. За последние три десятилетия криптография с открытым ключом стала неотъемлемым компонентом нашей глобальной цифровой инфраструктуры связи. Эти сети поддерживают множество приложений, которые важны для нашей экономики, нашей безопасности и нашего образа жизни, таких как мобильные телефоны, интернет-коммерция, социальные сети и облачные вычисления. В таком связанном мире способность людей, предприятий и правительств безопасно общаться, имеет первостепенное значение.

Ключевые слова: *Криптография, квантовая криптография, шифрование.*

Filippov M.A., Krotova E.L.

QUANTUM CRYPTOGRAPHY. ADVANTAGES AND DISADVANTAGES

The article is devoted to quantum cryptography, its differences from traditional cryptography. Special attention is paid to the advantages and disadvantages of quantum cryptography and its relevance in the modern world. Over the past three decades, public-key cryptography has become an integral component of our global digital communications infrastructure. These networks support many applications that are important to our economy, our security and our way of life, such as mobile phones, e-commerce, social networks and cloud computing. In such a connected world, the ability of people, businesses and governments to communicate securely is of paramount importance.

Keywords: *cryptography, quantum cryptography, encryption.*

Многие из наших наиболее важных коммуникационных протоколов основаны главным образом на трех основных криптографических функциях: шифрование с открытым ключом, цифровые подписи и обмен ключами. В настоящее время эти функции в основном реализуются с использованием обмена ключами Диффи-Хеллмана, криптосистемы RSA и криптосистемы эллиптической кривой. Их безопасность зависит от сложности определенных теоретико-числовых задач, таких как факторизация целых чисел или проблема дискретного журнала для разных групп. В скором времени начнут появляться квантовые компьютеры, новые технологии, использующие физические свойства материи и энергии для выполнения расчетов, которые смогут эффективно решать каждую из этих проблем, тем самым делая все криптосистемы с открытым ключом на основе таких допущений бесполезными в области защиты. Таким образом, достаточно мощный квантовый компьютер будет представлять угрозы безопасности многим формам современной коммуникации - от обмена ключами до шифрования и цифровой аутентификации. Долгое время методы разработки алгоритмов шифрования определялись только хитростью и изо-

бретательностью их создателей. И только в XX веке данной областью заинтересовались математики, а потом — и физики, что и привело к появлению квантовой криптографии[1].

Что такое квантовая криптография и её отличие от обычной криптографии

Классическая криптография решает фактически только две задачи: защиту передаваемых сообщений от прочтения и от модификации сторонними лицами. Она базируется на использование симметричных алгоритмов шифрования, в которых зашифровывание и расшифрование различаются лишь порядком исполнения и направлением некоторых простых шагов. Эти методы используют один и тот же скрытый элемент (ключ), и второе действие (расшифрование) является простым обращением первого (зашифрования). Поэтому любой из участников обмена может как зашифровать, так и расшифровать сообщение. По причине большой избыточности естественных языков непосредственно в зашифрованное сообщение очень тяжело внести осмысленное изменение, поэтому классическая криптография гарантирует также защиту от навязывания ложных данных. Если же естественной избыточности оказывается недостаточно для надежной защиты сообщения от модификации, она может быть искусственно увеличена методом добавления к нему особой контрольной комбинации. Если сказать вкратце, то защищённость классической криптографии строиться на уверенности в том, что злоумышленник не успеет за разумное время «взломать» шифр ввиду сложности используемых алгоритмов[2].

Квантовая криптография — способ защиты коммуникаций, основанный на определенных явлениях квантовой физики. В отличие от традиционной криптографии, которая использует математические способы, чтобы обеспечить секретность информации, квантовая криптография сконцентрирована на физике, изучая случаи, когда информация переносится с помощью объектов квантовой механики. Процесс отправки и приёма информации постоянно выполняется физическими средствами, например, при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи. А подслушивание может рассматриваться, как измерение определённых параметров физических объектов — в нашем случае, переносчиков информации. Обобщённо можно сказать, что защищённость квантовой криптографии выстраивается на утверждении о том, что никто не сможет «взломать» шифр, так как это противоречит физическим законам природы.

Преимущества и недостатки квантовой криптографии

К преимуществам квантовой криптографии можно отнести:

– Обнаружение пассивного перехватчика – атака злоумышленника вносит значительно больше ошибок, чем их возникает в квантовом канале в результате естественного шума.

– Теоретико-информационная стойкость распределения ключей – ключи, распределённые с помощью квантовых протоколов с теоретико-информационной стойкостью, используется для дальнейшего шифрования с использованием известных классических симметричных алгоритмов. Поэтому общий уровень стойкости криптосистемы повышается.

– Защищённость основана на фундаментальных физических законах и принципах.

– Однако также существуют недостатки:

– Не является полноценным завершённым решением защиты информации – необходима предварительная аутентификация пользователей; пользователи не имеющие никакого общего предустановленного начального секрета, не могут обменяться новым ключом для шифрования.

– С увеличением длины квантового канала значительно уменьшается скорость передачи – если длина канала >100 км, то скорость передачи составляет биты в секунду, хотя на расстояниях в 20-30 км уже достигают мегабитных скоростей.

– Деполяризация фотонов в квантовом канале приводит к достаточно высокому уровню естественных помех.

– Сложность реализации и высокая стоимость оборудования приводит к сильной конкуренции на рынке средств защиты информации, что в свою очередь заканчивается банкротством для небольших компаний3.

Заключение

Подводя итог, хотелось бы сказать, что последние разработки в области квантовой криптографии позволяют формировать системы, обеспечивающие фактически 100%-ю защиту ключа и информации. Используя знания по защите информации, как из классиче-

ской криптографии, так и из новейшей «квантовой» области, люди смогут получать результаты, превосходящие все известные криптографические системы4. Сегодняшняя квантовая криптография разработана с прицелом на будущее, в котором взлом классических шифров с открытым ключом может стать практически достижимым. Например, однажды квантовый компьютер сможет взломать сегодняшние шифры. Квантовая криптография также представляет собой прекрасный пример тесного взаимодействия между фундаментальными и прикладными исследованиями.

Литература:

1. Lily Chen Stephen Jordan Yi-Kai Liu Dustin Moody Rene Peralta Ray Perlner Daniel Smith-Tone "Report on Post-Quantum Cryptography", NISTIR 8105 DRAFT Phys. Rev. A, Vol. 15, 2016

2. Классическая и «современная» криптография. // Как устроен блочный шифр? URL: http://www.enlight.ru/crypto/articles/vino-kurov/blcyph_1.htm (дата обращения 09.06.2017)

3. Современные технологии квантовой защиты информации // DOCPLAYER. URL: http://docplayer.ru/38223070-Sovremennye-tehnologii-kvantovoy-zashchity-informacii.html (дата обращения 12.06.2017)

4. Квантовая криптография. // VIII Международная студенческая электронная научная конференция «Студенческий научный форму» - 2016 URL: https://www.scienceforum.ru/2016/1543/17525 (дата обращения 15.06.2017)

References

1. Lily Chen Stephen Jordan Yi-Kai Liu Dustin Moody Rene Peralta Ray Perlner Daniel Smith-Tone "Report on Post-Quantum Cryptography", NISTIR 8105 DRAFT Phys. Rev. A, Vol. 15, 2016.

2. Klassicheskaya i «sovremennaya» kriptografiya. // Kak ustroyen blochnyy shifr? URL: http://www.enlight.ru/crypto/articles/vino-kurov/blcyph_1.htm (data obrashcheniya 09.06.2017).

3. Sovremennyye tekhnologii kvantovoy zashchity informatsii // DOCPLAYER. URL: http://docplayer.ru/38223070-Sovremennye-tehnologii-kvantovoy-zashchity-informacii.html (data obrashcheniya 12.06.2017).

4. Kvantovaya kriptografiya. // VIII Mezhdunarodnaya studencheskaya elektronnaya nauchnaya konferentsiya «Studencheskiy nauchnyy formu» - 2016 URL: https://www.scienceforum.ru/2016/1543/17525 (data obrashcheniya 15.06.2017)

ФИЛИППОВ Михаил Александрович, студент кафедры Автоматики и телемеханики Пермского национального исследовательского политехнического университета. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: Misha-Fill@mail.ru

КРОТОВА Елена Львовна, кандидат физико-математических наук, кафедра Высшей математики Пермского национального исследовательского политехнического университета, доцент. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

FILIPPOV Mikhail, student of the Department of Automation and Telemechanics of the Perm National Research Polytechnic University. 614990, Permsky Kray, Perm, Komsomolsky Prospekt, 29. E-mail: Misha-Fill@mail.ru

KROTOVA Elena, candidate of physico-mathematical sciences, Department of Higher mathematics, Perm National Research Polytechnic University, docent. 614990, Permsky Kray, Perm, Komsomolsky prospekt, 29. E-mail: lenkakrotova@yandex.ru

УДК 004:338 + 004.738.5:336.743 Вестник УрФО № 4(26) / 2017, с. 28–30

Осипов Н. Р., Кротова Е. Л.

ТЕХНОЛОГИЯ БЛОКЧЕЙН. ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

В последнее время многие из нас все чаще сталкиваются с таким понятием, как блокчейн. Это что за система? К сожалению, знают об этом далеко не все, хотя она имеет весьма перспективные шансы на развитие и внедрение в повседневную жизнь. Блокчейн в переводе с английского - цепочка блоков, но что это значит? Это непрерывная цепочка блоков информации, выстроенная по определенным правилам. Чаще всего услышать термин «блокчейн» можно, когда речь идет о транзакциях в различных криптовалютах, однако в блоках может содержаться любая информация. Рассмотрим подробнее актуальность этой технологии, её применимость в современной жизни, а также её преимущества и недостатки.

Ключевые слова: *Блокчейн, криптовалюта, цепочки блоков транзакций, биткоин.*

Osipov N. R., Krotova E. L.

TECHNOLOGY OF BLOCKCHAIN. ADVANTAGES AND DISADVANTAGES

Recently, many of us are increasingly confronted with such a concept as a blockchain. What kind of system is this? Unfortunately, not everyone knows this, although it has very promising chances for development and implementation in everyday life. Blockchain is translated from English - a chain of blocks, but what does this mean? This is a continuous chain of information blocks, built according to certain rules. Most often, the term "blockchain" can be heard when it comes to transactions in various crypto-currencies, however, any information can be contained in the blocks. Let's consider in more detail the relevance of this technology, its applicability in modern life, as well as its advantages and disadvantages.

Keywords: *Blockchain, crypto currency, chains of transaction blocks, bitcoin.*

Актуальность блокчейна

Понятие блокчейн обозначает технологию распределенного хранения блоков данных, которые связываются в упорядоченные цепочки. Сегодня Блокчейн внедряется во многие интернет-системы, потому что эта технология обеспечивает достоверность и защищенность сохраненных сведений. Общедоступность и одновременно 100% безопасность блокчейн обеспечивается:

– Сложными математическими алгоритмами;

– Специальными программами шифрования;

– Пятью тысячами мощных компьютеров, включенных в систему майнинга, между которыми распределена вся совокупность данных.

Взломать такую систему теоретически возможно, зато практически – совершенно бессмысленно, так как никакой доход заведомо не покроет огромных расходов на глобальную атаку.

Сущность «цепи блоков» как общедоступной, распределенной и 100% достоверной базы данных делает применение блокчейн весьма привлекательным для компаний, работающих в разных областях[1].

В настоящее время уже существует ряд расширений для разработки бизнес-приложений на блокчейн, обеспечивающих:

– безопасное администрирование сетей, исключающее хакерские атаки MITM («человек посередине») и снимающее проблему «единого администратора»;

– хранение цифровых сертификатов, делающее полностью защищенным доступ пользователей к сайтам (в частности, исключая перехват паролей);

– безопасные двусторонние сделки без привлечения гарантирующей третьей стороны (юридической фирмы, нотариуса, банка и др.);

– фиксацию времени размещения документов, позволяющую решать вопросы патентования, авторского права и др.;

– подтверждение подлинности продукта (товара) с помощью надежно защищенного сертификата;

– подтверждение прав на любую собственность;

– создание общедоступных электронных визиток, информация на которых автоматически обновляется даже после «раздачи» по интернет-ресурсам;

– систему DNS, неуязвимую для DDOS-атак,

– и другое.

Преимущества и недостатки

Блокчейн сегодня не просто новый способ работы с информацией, который придумали IT - специалисты для своих узких нужд. Эксперты считают, что внедрение этой технологии по возможному эффекту не уступает открытию Интернета. Итак, рассмотрим преимущества технологии блокчейн[5]:

1. Представленная технология помогает заниматься торговлей, внедрить разные сервисы в жизни и даже изменить работу банковской сферы.

2. Суть блокчейна базируется на прозрачности и безопасности, поэтому не стоит беспокоиться о возможных подвохах.

3. Используя данную систему можно избежать коррупции, которая часто становится существенной преградой для развития.

4. Можно создать свой блокчейн альянс, в который будут входить поставщики, партнеры и даже конкуренты.

Но при всех своих плюсах у этой технологии есть и минусы, поскольку система только развивается:

1. Производительность блокчейна ниже, если сравнивать ее с высоконагруженными системами.

2. Пока еще сложно найти разработчиков, которые бы быстро и без ошибок справились с работой. К тому же для поддержания системы необходимы специалисты, которых также мало.

3. Критика блокчейн касается и того, что необходимы большие инвестиции в инфраструктуру, то есть безопасность, систему хранения приватных ключей и так далее.

Возможность использования в будущем, актуально или нет

Вполне возможно, что сейчас – именно то время, когда технология проходит обкатку вживую на весьма значимых областях общественной жизни, и в скором времени мы увидим все больше и больше проектов и платформ, использующих блокчейн. Уже сейчас банки пытаются активно внедрять это у себя (в том числе и для снижения операционных расходов), на рынке появляются все новые и новые игроки, стремящиеся популяризовать использование технологии. Новые проекты на блокчейне будут основываться на его главных преимуществах – открытости, защищенности, безопасности.

На финансовом рынке значительно изменятся роли участников рынка, а также их бизнес-модели[1]:

У *клиентов* институтов финансового рынка появится ряд преимуществ, включая снижение операционных издержек и стоимости обслуживания ценных бумаг. Мелкие и крупные инвесторы смогут эффективнее взаимодействовать друг с другом, а сделки станут быстрее, надежнее и безопаснее.

Дилеры все еще будут играть важную роль на рынке, обеспечивая ликвидность активов, а также принимая на себя основные риски в случае низкой ликвидности. Однако, теперь основной их задачей не будет являться обеспечение доступа на рынок, а, скорее, консультирование по вопросам сделок и управление их исполнением.

Центральная клиринговая палата. Для операций с активами за наличный расчет, осуществляемых в режиме реального времени, централизованный клиринг сделки больше не потребуется, так как обе стороны еще до заключения сделки будут знать о возможностях другой стороны исполнить свои обязательства, а расчеты будут осуществляться практически мгновенно.

Всего за несколько лет блокчейн уже прошел путь от новинки в технологическом мире до инструмента, которым начинают пользоваться крупные банки, корпорации и государства.

Заключение

Из всего сказанного следует, что технология блокчейн отличный инструмент для хранения данных о правах собственности, юридических обязательствах, финансовых операциях и при этом обеспечивает всеобщую доступность для ознакомления и абсолютную прозрачность. Также обеспечивается надежная защита от подлога любого вида, различных взломов и каких бы то ни было несанкционированных вмешательств.

Упрощая можно сказать, что технология блокчейн - это сейф с прозрачными стенами и камерой наблюдения, то есть в него можно положить что-либо, но при этом любой наблюдатель заметит попытку подмены или видоизменения содержимого.

Литература

1. Как блокчейн изменит финансовый рынок // forklog URL: http://forklog.com/kak-blokchejn-izmenit-finansovyj-rynok/ (дата обращения 20.06.2017)

2. Что такое технология блокчейн и как она работает? // Woman advice URL: http://womanadvice.ru/chto-takoe-blokcheyn-tehnologiya-i-kak-ona-rabotaet (дата обращения 20.06.2017)

3. Различия, достоинства, недостатки: публичные и приватные блокчейны // Хабрахабр URL: https://habrahabr.ru/company/bitfury/blog/324458/ (дата обращения 27.06.2017)

4. Что такое блокчейн? Преимущества и недостатки технологии // Демидыч URL: https://deminv.ru/investitsii-v-kriptovalyutu/kriptovaluti/188-chto-takoe-bictoin-cash (дата обращения 10.08.2017)

5. Преимущества и недостатки технологии блокчейн // YaUmma.ru URL: http://yaumma.ru/science/2017/08/23/preimuschestva-i-nedostatki-tehnologii-blokcheyn.html (дата обращения 25.08.2017)

References

1. Kak blokcheyn izmenit finansovyy rynok // forklog URL: http://forklog.com/kak-blokchejn-izmenit-finansovyj-rynok/ (data obrashcheniya 20.06.2017).

2. Chto takoye tekhnologiya blokcheyn i kak ona rabotayet? // Woman advice URL: http://womanadvice.ru/chto-takoe-blokcheyn-tehnologiya-i-kak-ona-rabotaet (data obrashcheniya 20.06.2017).

3. Razlichiya, dostoinstva, nedostatki: publichnyye i privatnyye blokcheyny // Khabrakhabr URL: https://habrahabr.ru/company/bitfury/blog/324458/ (data obrashcheniya 27.06.2017).

4. Chto takoye blokcheyn? Preimushchestva i nedostatki tekhnologii // Demidych URL: https://deminv.ru/investitsii-v-kriptovalyutu/kriptovaluti/188-chto-takoe-bictoin-cash (data obrashcheniya 10.08.2017).

5. Preimushchestva i nedostatki tekhnologii blokcheyn // YaUmma.ru URL: http://yaumma.ru/science/2017/08/23/preimuschestva-i-nedostatki-tehnologii-blokcheyn.html (data obrashcheniya 25.08.2017).

ОСИПОВ Никита Романович, студент кафедры Автоматики и телемеханики Пермского национального исследовательского политехнического университета. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: nikita.osipov.96@yandex.ru

КРОТОВА Елена Львовна, кандидат физико-математических наук, кафедра Высшей математики Пермского национального исследовательского политехнического университета, доцент. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

OSIPOV Nikita, student of the Department of Automation and Telemechanics of the Perm National Research Polytechnic University. 29 Komsomolsky prospekt, Perm, Perm krai, Russia, 614990. E-mail: nikita.osipov.96@yandex.ru

KROTOVA Elena, candidate of physico-mathematical sciences, Department of Higher mathematics, Perm National Research Polytechnic University, docent. 29 Komsomolsky prospekt, Perm, Perm krai, Russia, 614990. E-mail: lenkakrotova@yandex.ru

УДК 003.26 + 004.056.55 + 004.22 Вестник УрФО № 4(26) / 2017, с. 31–35

Филиппов М. А., Кротова Е. Л.

КВАНТОВАЯ КРИПТОГРАФИЯ. ПРОТОКОЛЫ КВАНТОВОЙ КРИПТОГРАФИИ

В этой статье представлен обзор распределения квантовых ключей, ориентированного на сферу информационных технологий. В частности, в этой статье описывается протокол BB84 и его многочисленные варианты, а также произведён их сравнительный анализ. Привлекательность идеи квантовой криптографии состоит в разработке *новейшего способа генерирования полностью случайных скрытых ключей между пользователями квантовой линии связи, которые раньше никогда не встречались и не имеют общей скрытой информации. Секретность способа и невозможность незаметного съема информации с линии связи основаны на законах квантовой физики — в противоположность используемым в настоящее время способам криптографии, которые основаны на математических закономерностях и поддаются расшифровке.*

Ключевые слова: *Криптография, квантовая криптография, протокол, BB84, B92, BB84 (4+2), E91, шифрование.*

Filippov M. A., Krotova E. L.

QUANTUM CRYPTOGRAPHY. PROTOCOLS OF QUANTUM CRYPTOGRAPHY

This article presents an overview of the distribution of quantum keys oriented to the sphere of information technologies. In particular, this article describes the BB84 protocol and its numerous variants, as well as their comparative analysis. The attraction of the idea of quantum cryptography is the development of the newest way to generate completely random hidden keys between users of the quantum communication line, which previously never met and do not have common hidden information. The secrecy of the method and the impossibility of unnoticeable retrieval of information from the communication line are based on the laws of quantum physics - in contrast to the currently used cryptography methods, which are based on mathematical laws and can be deciphered.

Keywords: *Cryptography, quantum cryptography, protocol, BB84, B92, BB84 (4 + 2), E91, encryption.*

Что такое протокол BB и принцип работы

Существует множество протоколов квантовой криптографии основанных на передаче информации посредством кодирования в состояниях одиночных фотонов, например: BB84, B92, BB84 (4+2) и их модификации. Кроме того, существует протокол, разработанный для кодирования информации в спутанных состояниях – E91.

BB84 — первый протокол квантового рас-

пределения ключа, который был предложен в 1984 году Чарльзом Беннетом и Жилем Брассаром. Он основан на идеях поляризации фотонов. Ключ состоит из битов, которые передаются как фотоны.

При рассмотрении протокола будем называть отправителя Алисой, а получателя Бобом. Сегодня у них есть по сути два варианта: встретиться и сообща сгенерировать криптографический ключ (надеясь, что никто его не подсмотрит) или использовать протоколы с открытым ключом, такой как RSA.

Первый вариант не особо удобен - ключ надо постоянно обновлять (чем дольше используем один и тот же ключ, тем больше шансов, что его кто-то узнает).

Второй вариант используется повсеместно, но, если будет создан квантовый компьютер с адекватным набором элементов, протокол RSA станет уязвим.

Тут в дело и вступает протокол BB84. Что же нужно для того, чтобы он заработал? У Алисы и Боба есть два канала связи: открытый и закрытый. Закрытый канал используется для генерации ключа, открытый - для передачи зашифрованной информации. Открытый канал должен быть устроен так, что, хотя прослушивать его могут все и вся, изменений в передаваемую информацию не может вносить никто. Что касается закрытого канала - необходимо следить, чтобы его никто не прослушивал (и протокол BB84 с этим справляется). Разберём более подробно прокол BB84, позволяющим двум пользователям создать общий криптографический ключ[1].

В протоколе BB84 используются 4 квантовых состояния фотонов, как представлено на рисунке 1, например направление вектора поляризации одно из которых Алиса выбирает в зависимости от передаваемого бита: 90° или 135° для «1», 45° или 0° для «0».

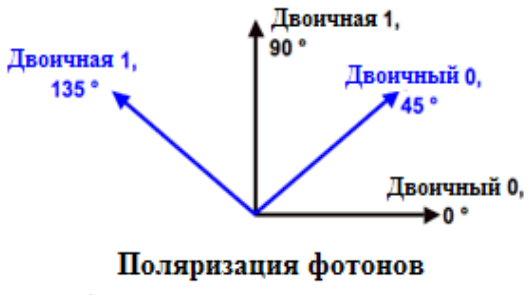

Рисунок 1 – Поляризация состояний в протоколе BB84

Одна пара квантовых состояний принадлежит базису «+». Другая пара квантовых состояний принадлежит базису «×» (рисунок 2). Внутри обоих базисов состояния ортогональны, но состояния из разных базисов являются попарно неортогональными (неортогональность необходима для попыток съёма информации)[4].

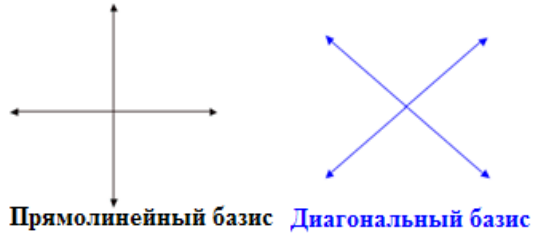

Рисунок 2 – Базисы квантовых состояний

Этапы генерации общего ключа:

Для генерации ключа отправитель пропускает фотоны через четыре традиционных однонаправленных фильтра (линейных поляризатора). Получатель для определения посылаемых бит (поляризации фотонов) применяет две поляризационные разделительные призмы, работающие в прямолинейном и диагональном базисах.

Рассмотрим ситуацию, когда Алиса и Боб передают информацию без прослушивания на примере таблицы 1:

1. Алиса генерирует случайную последовательность бит и для каждого из них случайным образом выбирает один из двух базисов. Полученные фотоны посылает Бобу

2. Боб получает фотоны и считывает их случайным образом, чередуя базисы, т.к. он не знает какую последовательность базисов выбрала Алиса. Некоторые базисы будут правильно отгаданы.

3. Боб открыто сообщает Алисе порядок использования им базисов.

4. Алиса открыто сообщает Бобу, какие базисы были выбраны Бобом правильно, те базисы, которые совпали, формируют ключ.

5. Биты для правильно выбранных базисов используются для проверки целостности переданных данных и формирования ключа. В оригинальном протоколе BB84 из этих «правильных» битов выбирается определенная часть и открыто сравнивается. В случае совпадения (канал не прослушивается и данные дошли без искажений), биты, которые открыто сравнивались, удаляются из ключа и оставшаяся часть используется для формирования ключа требуемой длины[3].

Рассмотрим другую ситуацию, когда пе-

Таблица 1

Пример обмена ключами по протоколу BB84

Этапы									
	1	Случайным образом сгенерированные биты	1	0	0	1	1	1	0
		Базис, выбранный Алисой	×	×	+	×	+	+	+
		Фотоны	\	/	–	\	|	|	–
	2	Базис, выбранный Бобом	+	×	×	+	+	+	×
		Биты, определенные Бобом	0	0	1	0	1	1	1
	3,4	Проверка правильности применения базисов Бобом		V			V	V	
	5	Биты для контроля целостности и формирования ключа		0			1	1	

редаваемую информацию между Алисой и Бобом хочет подслушать злоумышленник (будем именовать Евой):

Как раньше было сказано, в среднем половина посланных Алисой фотонов отбрасывается за счёт того, что Боб выбрал не тот базис. Дальше рассматриваются «правильные» фотоны. Ева перехватывает «правильный» фотон, выбирает базис и посылает этот фотон Бобу. С вероятностью 50% она выберет правильный базис, тем самым получая правильный ответ и пересылает дальше правильный фотон. Но с той же самой вероятностью она выбирает неправильный базис, получает случайный ответ и посылает дальше заведомо ложный фотон. Боб же, выбирая для этого фотона базис, с вероятностью 50% получит правильный ответ, который послала Алиса.

Получается, что при вмешательстве, Ева с вероятностью 50% не меняет ничего, а в половине случаев из оставшихся 50% Боб всё равно получает правильный ответ. Таким образом, Ева вносит изменения в четверть битов ключа. Алиса и Боб подозревают, что их общение подслушивается, и жертвуют частью ключа и сверяют по открытому каналу. Если обнаружено несовпадение в 25% случаев, то их общение становится небезопасным.

Модификации протокола BB и их сравнительный анализ

Протокол B92

В 1992 году Чарльз Беннетт предложил, по сути, упрощенный вариант BB84. Основное различие в B92 заключается в том, что необходимы только два состояния, а не возможные 4 поляризационных состояния в BB84. Как показано на рисунке 3, «0» может быть закодирован, как 0 градусов в прямолинейной основе и «1» может быть закодирована на 45 градусов по диагонали. Как и BB84, Алиса передает Бобу строку фотонов, закодированную со случайно выбранными битами, но на этот раз Алиса диктует, какие базисы она должна использовать. Боб все еще случайно выбирает базисы, но если он выбирает неправильный базис, он ничего не будет менять. Боб может говорить Алисе после каждого бита, который она отправляет, правильно ли он выбрал базис.

Рисунок 3 – Поляризация состояний в протоколе B92

Протокол BB84 (4+2)

Данный протокол является промежуточным между протоколами BB84 и B92. В протоколе используются 4 квантовых состояния для кодирования «0» и «1» в двух базисах. Состояния в каждом базисе выбираются неортогональными, состояния в разных базисах также попарно неортогональны (рисунок 4).

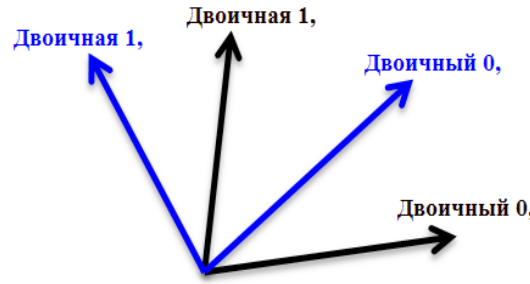

Рисунок 4 – Поляризация состояний в протоколе BB84 (4+2)

Процесс генерации ключа точно такой же как и в протоколе BB84, который описан выше[4].

Протокол E91

В протоколе используются пары фотонов, рождающиеся в антисимметричных поляризационных состояниях.

Отправитель генерирует некоторое количество фотонных пар. Один фотон из каждой пары он оставляет для себя, второй посылает своему партнеру. При получении отправителем значения поляризации «1», его партнер зарегистрирует значение «0» и наоборот. Ясно, что таким образом партнеры всякий раз, могут получить идентичные псевдослучайные кодовые последовательности.

Предположим, что изначально создастся некоторое количество пар фотонов максимально запутанных, затем один фотон из каждой пары посылается Алисе, а другой Бобу. Тогда образуется три возможных квантовых состояния для этих пар. Каждое из этих трёх состояний кодирует биты «0» и «1» в уникальном базисе. Затем Алиса и Боб осуществляют измерения на своих частях разделённых пар фотонов, применяя соответствующие приборы. Алиса записывает измеренные биты, а Боб записывает их дополнения до 1. Результаты измерений, в которых пользователи выбрали одинаковые базисы, формируют «сырой» ключ. Для остальных результатов Алиса и Боб проводят проверку на присутствие Евы[5].

Заключение

В заключении хотелось бы сказать, что квантовая криптография - очень перспективная часть криптографии, ведь технологии, используемые там, позволяют вывести безопасность информации на высочайший уровень. Интерес к квантовой криптографии со стороны коммерческих и военных организаций растет, так как эта технология гарантирует абсолютную защиту. Создатели технологий квантовой криптографии вплотную приблизились к тому, чтобы выпустить их из лабораторий на рынок. Осталось немного подождать, и уже очень скоро квантовая криптография обеспечит еще один слой безопасности для нуждающихся в этом организаций.

Литература

1. Квантовая криптография. // TRENDCLUB. URL: http://trendclub.ru/365 (дата обращения 16.06.2017)

2. A Survey of the Prominent Quantum Key Distribution Protocols // QKD. URL: http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#b92 (дата обращения 13.06.2017)

3. BB84 // Википедия. URL: https://ru.wikipedia.org/wiki/BB84 (дата обращения 15.06.2017)

4. Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю. Квантовая криптография учебное пособие / под ред. МАКС Пресс – 2011. – С. 112.

5. О квантовой криптографии. Проктоколы E91 & Lo05 // Хабрахабр. URL: https://habrahabr.ru/post/316252/ (дата обращения 15.06.2017)

References

1. Kvantovaya kriptografiya. // TRENDCLUB. URL: http://trendclub.ru/365 (data obrashcheniya 16.06.2017).

2. A Survey of the Prominent Quantum Key Distribution Protocols // QKD. URL: http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#b92 (data obrashcheniya 13.06.2017.

3. VV84 // Vikipediya. URL: https://ru.wikipedia.org/wiki/BB84 (data obrashcheniya 15.06.2017).

4. Kronberg D.A., Ozhigov YU.I., Chernyavskiy A.YU. Kvantovaya kriptografiya uchebnoye posobiye / pod red. MAKS Press – 2011. – S. 112.

5. O kvantovoy kriptografii. Proktokoly E91 & Lo05 // Khabrakhabr. URL: https://habrahabr.ru/post/316252/ (data obrashcheniya 15.06.2017).

ФИЛИППОВ Михаил Александрович, студент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: Misha-Fill@mail.ru

КРОТОВА Елена Львовна, кандидат физико-математических наук, кафедра «Высшей математики» Пермского национального исследовательского политехнического университета. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

FILIPPOV Mikhail, student of the Department of Automation and Telemechanics of the Perm National Research Polytechnic University. 614990, Permsky Kray, Perm, Komsomolsky Prospekt, 29. E-mail: Misha-Fill@mail.ru

KROTOVA Elena, candidate of physico-mathematical sciences, Department of Higher mathematics, Perm National Research Polytechnic University, docent. 614990, Permsky Kray, Perm, Komsomolsky Prospekt, 29. E-mail: lenkakrotova@yandex.ru

УДК 004.056.5 + 621.391.2:004.056.5 Вестник УрФО № 4(26) / 2017, с. 36–40

Пономарева Ю. В., Минбалеев А. В.

ПРОБЛЕМЫ ОЦЕНОЧНОСТИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

В статье рассмотрены вопросы ограничения распространения отдельных видов информации и проблемы правового регулирования ограничений. Авторами особое внимание уделено проблеме разъяснений контролирующих органов, дающих расширительное толкование запретов и ограничений, устанавливаемых в законе. Сделан вывод об отсутствии единого и полного перечня информации, распространение которой запрещено, а также однозначных критериев ее оценки.

Поднимается проблема субъективности восприятия той или иной публикуемой информации, что обусловлено оценочным характером многих видов информации ограниченного распространения, отсутствием методических рекомендаций по определению факта распространения той или иной информации ограниченного распространения. В результате многие СМИ вынуждены отказываться от освещения острых и актуальных социальных тем во избежание рисков привлечения к административной ответственности, в том числе во избежание блокировки интернет-ресурсов, получения предписания со стороны органов власти или даже прекращения регистрации в качестве СМИ. Делается вывод, что расширение перечня информации ограниченного распространения должно осуществляться с учетом детального общественного обсуждения данной необходимости.

Ключевые слова: *запрещенная информация, вредная информация, информация ограниченного распространения.*

PROBLEMS OF THE ESTIMATION OF THE LIMITED DISTRIBUTION INFORMATION

The article considers the issues of restricting the dissemination of certain types of information and the problem of legal regulation of restrictions. The authors pay special attention to the problem of clarifying the controlling bodies, which give an extensive interpretation of the prohibitions and restrictions established in the law. It is concluded that there is no single and complete list of information, the dissemination of which is prohibited, as well as unambiguous criteria for its evaluation.

The problem of subjectivity of perception of this or that published information is raised, which is caused by the estimated nature of many types of information of limited distribution, the absence of methodological recommendations for determining the dissemination of some information of limited dissemination. As a result, many media outlets have to refuse to cover acute and urgent social topics in order to avoid risks of administrative liability, including to avoid blocking Internet resources, getting orders from the authorities or even stopping registration as media. It is concluded that the expansion of the list of information of limited dissemination should be carried out taking into account a detailed public discussion of this need.

Keywords: *forbidden information, harmful information, the information of limited distribution.*

Ст. 29 Конституции Российской Федерации устанавливает право на информацию в формулировке, закрепляя, что «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом». Сама структура нормы предусматривает фактически лишь одно изъятие из права – доступ к сведениям, составляющим государственную тайну. Во втором пункте дается такое ограничение свободы слова как запрет пропаганды или агитации, возбуждающей социальную, расовую, национальную или религиозную ненависть и вражду, пропаганда социального, расового, национального, религиозного или языкового превосходства. Иных ограничений на доступ и распространение информации не приводится. Вместе с тем, с каждым годом растет количество нормативных правовых актов, которые вводят новые виды информации, доступ к которым ограничивается либо распространение которых запрещается.

Ранее было целесообразно проводить классификацию информации на общедоступную и информацию ограниченного доступа, в состав которой включалась и «вредная» информация. Сейчас же, ввиду увеличения объема правовых норм, которые устанавливают ограничение на распространение различных видов информации, формируется отдельный блок информации – информации ограниченного распространения, правовой режим которой кардинально отличается от информации ограниченного доступа.

В отношении информации ограниченного распространения нет мер охраны информации, нет специальных субъектов (за исключением ограничений, предусмотренных законодательством о средствах массовой информации), обязанных защищать информацию, нет зачастую четко обозначенных критериев такой информации. В отношении такой информации законодатель предусматривает запрет на ее распространение, а также ответственность за ее распространение.

В настоящее время интерес исследователей направлен на систематизацию и приведение полного перечня таких сведений либо на порядок ограничения доступа к интернет-ре-

сурсам, на которых были размещены указанные сведения. Вместе с тем, следует отметить, что на настоящий момент не представляется даже возможным указать полный перечень такой информации ограниченного распространения по двум причинам. Во-первых, в связи с оценочным характером ряда понятий (такие как «пропаганда», «агитация», «явное неуважение к обществу»). Такие оценочные категории дают большую свободу для правоприменителя и, как следствие, для злоупотребления такой свободой. Так, в частности, в постановлении Конституционного Суда РФ от 23 сентября 2014 № 24-П «По делу о проверке конституционности ч. 1 ст. 6.21 Кодекса Российской Федерации об административных правонарушениях в связи с жалобой граждан Н.А. Алексеева, Я.Н. Евтушенко и Д.А. Исакова» была сделана попытка дать определение понятию «пропаганда», однако суд дал сразу несколько определений этому процессу, которые мало согласуются между собой.

Помимо разъяснений оценочных понятий судом, существуют законодательные попытки выделения критериев определения информации, распространение которой ограничено. Так, в отношении информации о детской порнографии, наркотических средствах и суицидах были разработаны критерии, утвержденные совместным приказом Роскомнадзора № 1022, ФСКН России № 368, Роспотребнадзора № 666 от 11 сентября 2013 г. «Об утверждении критериев оценки материалов и (или) информации, необходимых для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службой Российской Федерации по контролю за оборотом наркотиков, Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека о включении доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие запрещенную информацию, в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (далее – Приказ 1022/368/666). Вместе с тем, возникают вопросы относительно законности принятия такого приказа и обоснованности введения им критериев, которые являются расширительным толкованием норм закона. Рассмотрим юридический статус данного документа.

Федеральный закон «Об информации, информационных технологиях и о защите информации» в ст. 15.1 отсылает к постановлению Правительства РФ в части определения порядка принятия решений уполномоченных Правительством РФ федеральных органов исполнительной власти о включении доменного имени в Единый реестр, принимаемые в соответствии с их компетенцией. Само постановление Правительства РФ от 26 октября 2012 г. №1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» определяет порядок отнесения уполномоченными органами, но указывает, что критерии разрабатываются Роскомнадзором в отношении материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера, распространяемых посредством сети «Интернет», Министерством внутренних дел РФ в отношении информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, а также о способах и местах культивирования наркосодержащих растений, Федеральной налоговой службой в отношении информации, содержащей пропаганду азартных игр, Роспотребнадзором в отношении информации о способах совершения самоубийства, а также призывов к совершению самоубийства.

В то же время Приказ 1022/368/666разработан Роспотребнадзором, ФСКН, Роскомнадзором, соответственно, критерии в отношении информации о наркотических, психотропных средствах и их прекурсоров разра-

ботаны неуполномоченным органом, а принятие такого приказа иными органами государственной власти выходит за пределы их полномочий или компетенций. Так, в положении о Роскомнадзоре указывается, что Федеральная служба может издавать акты ненормативного характера. В положении о Роспотребнадзоре указано, что служба издает приказы по вопросам, отнесенным к компетенции службы. При этом вопрос ограничения доступа к информации к компетенции службы само положение не относит, этот вопрос отнесен к компетенции службы только постановлением Правительства №1101. Федеральная служба по контролю за оборотом наркотиков являлся неуполномоченным органом, который в соответствии с постановлением №1101 должен был разрабатывать критерии. А в соответствии с положением о данной службе директор издавал нормативные правовые акты, которые, исходя из прямого толкования норм, действовали именно в рамках Федеральной службы по контролю за оборотом наркотиков, а не носили общеобязательный характер. Таким образом, юридический статус указанного документа с точки зрения порядка принятия и субъектов нормотворчества остается неопределенным.

Вместе с тем, решение этого вопроса крайне важно, поскольку федеральными законами установлен прямой запрет на пропаганду наркотиков и распространение информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений. В то же время в Приказе 1022/368/666 дано более пространное понимание информации о наркотических средствах, в том числе информация о способах ухода от уголовной и административной ответственности за правонарушения, связанные с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров; информация о местах приобретения, ценах и способах получения тех или иных видов наркотических средств, психотропных веществ и их прекурсоров (в том числе с использованием их сленговых наименований); информация, направленная на формирование у целевой аудитории положительного образа лиц, осуществляющих изготовление, разработку и использование наркотических средств, психотропных веществ и их прекурсоров, предоставляющих услуги по их приобретению либо осуществляющих культивирование растений, содержащих наркотические средства, психотропные и их прекурсоры (за исключением художественных произведений, в которых описывается информация, оправданная их жанром).

Тем самым, происходит бессистемное ограничение доступа к определенным видам информации на уровне подзаконных нормативных актов, что негативно отражается на защите права на информацию.

Еще одним спорным моментом расширительного толкования на запрет публикации информации о способах самоубийства и призывах к его совершению. Так, Приказ 1022/368/666 квалифицирует как призыв к совершению самоубийства в том числе «приведение конкретных примеров, представляющих собой популяризацию конкретных действий других людей, которые уже совершили самоубийство» – такая формулировка фактически дает возможность широкого толкования такого положения, при котором любое описание самоубийств даже в исторических аспектах может быть расценено как популяризация конкретных действий. Так, в частности, даже статья об исторических случаях массового самоубийства расценивается как нарушающая требования законодательства.

Второй причиной того, что невозможно указать полный перечень информации, распространение которой запрещено, является отнесение законодателем к основанию ограничения на распространение информации решение суда о признании информации, распространяемой посредством сети «Интернет», информацией, распространение которой в Российской Федерации запрещено как отдельного основания.

На первый взгляд, утверждение о том, что случай признания информации информацией, распространение которой в Российской Федерации запрещено, нельзя отнести к самостоятельному основанию для ограничения доступа к информации, однако, как показывает судебная практика, такое основание вполне может стать самостоятельным и фактически сделать список информации ограниченного распространения открытым.

Так, в одном из судебных решений суд пришел к выводу о том, что распространение информации о способах совершения коррупционных преступлений также является ин-

формацией, распространение которой должно быть запрещено (Апелляционное определение Кировского областного суда от 15.05.2014 по делу № 33-1578/2014). Прокурор обосновал свою позицию тем, что правоотношения, вытекающие из федеральных законов «О противодействии экстремистской деятельности» и «О противодействии коррупции в Российской Федерации», являются сходными применительно к целям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Таким образом, подобные судебные решения дают предпосылку для формирования определенной практики по запрещению распространения информации, распространение которой прямо не запрещено законодателем.

Еще одной существенной проблемой, на наш взгляд, является субъективность восприятия той или иной публикуемой информации. Это также обусловлено оценочностью многих видов информации ограниченного распространения, отсутствием методических рекомендаций по определению факта распространения той или иной информации ограниченного распространения. В результате многие СМИ вынуждены отказываться от освещения острых и актуальных социальных тем во избежание рисков привлечения к административной ответственности, в том числе во избежание блокировки интернет-ресурсов, получения предписания со стороны Роскомнадзора или даже прекращения регистрации в качестве СМИ. На наш взгляд, расширение перечня информации ограниченного распространения должно осуществляться с учетом детального общественного обсуждения данной необходимости. Введение запретов на распространение информации во многом негативно сказывается на развитии гражданского общества, в котором люди способны самостоятельно оценивать информацию, ее ценность и на основании ее анализа принимать взвешенные решения.

ПОНОМАРЕВА Юлия Владимировна, юрисконсульт ООО «Рамблер БС», соискатель кафедры теории государства и права, конституционного и административного права Южно-Уральского государственного университета (национального исследовательского университета). 454080, г. Челябинск, пр. Ленина, 76. E-mail: julia.ponomareva17@mail.ru.

МИНБАЛЕЕВ Алексей Владимирович, профессор кафедры теории государства и права, конституционного и административного права, заместитель директора Юридического института Южно-Уральского государственного университета (национального исследовательского университета), доктор юридических наук, доцент. E-mail: minbaleevav@susu.ru

PONOMAREVA Yulia, legal adviser, Rambler, LLC, competitor of the Department of Theory of State and Law, Constitutional and Administrative Law of the South Ural State University (National Research University). 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: julia.ponomareva17@mail.ru

MINBALEEV Aleksey, Professor of the Department of Theory of State and Law, Constitutional and Administrative Law, Deputy Director of the Law Institute of the South Ural State University (National Research University), Doctor of Law, assistant professor. 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: minbaleevav@susu.ru

УДК 004:34.03 Вестник УрФО № 4(26) / 2017, с. 41–44

Чубукова С. Г.

К ВОПРОСУ О ПРАВОВОМ РЕГУЛИРОВАНИИ ИНФОРМАЦИОННЫХ СИСТЕМ

В статье рассматривается регулирование информационных систем, в том числе, государственных информационных систем и информационных систем местного самоуправления в современных условиях - внедрении цифровой экономики, распространении облачных технологий и основанных на них информационных систем, технологии блокчейн и т.д. Поскольку информационные системы представляют собой сложноорганизованный объект со множеством подсистем и большим количеством информационных потоков, необходимо обеспечивать правовое регулирование каждого из этапов жизненного цикла информационных систем для реализации функций информационной системы и избежания состояний неэффективности информационной системы.

Ключевые слова: *правовое регулирование, информационная система, жизненный цикл информационных систем.*

Chubukova S. G.

THE ISSUE OF LEGAL REGULATION OF INFORMATION SYSTEMS

The article is devoted to the regulation of information systems, including state information systems and information systems of local self-government in modern conditions-the introduction of the digital economy, the dissemination of cloud technologies and information systems based on them, block chain technology, etc. Since information systems are a complex organization with a multitude of subsystems and a large number of information flows, it is necessary to ensure the legal regulation of each stage of the life cycle of information systems to realize the functions of the information system and to avoid states of inefficiency in the information system.

Keywords: *legal regulation, information system, life cycle of information systems*

Информационные системы и технологии играют незаменимую роль в обеспечении всех аспектов деятельности государства, в частности, деятельности государственных органов и органов местного самоуправления. Тренды в информационном мире таковы, что организации должны минимизировать затраты, связанные с получением, обработкой и хранением информации. Учитывая, что объемы обрабатываемых данных возрастают с каждым периодом времени, необходимо обеспечивать корректную и сопоставимую с ценностью данных организацию информационных процессов и потоков информации. Информационные системы в целом представляют собой сложный объект, созданный для реализации действий с информацией, и направленный и получение обработанной и полезной информации.

Учитывая в данный момент повсемест-

ную цифровизацию деятельности как органов государственной власти, местного самоуправления, так и частных коммерческих организаций, необходимо уделить внимание существующей информационной инфраструктуре, информационному фундаменту, которым на сегодняшний день, в большинстве случаев, являются локальные или сетевые информационные системы. За последнее время внимание государства к информационным технологиям непомерно возросло. Это связано с развивающимися во всем мире технологией блокчейн, развитием «интернета вещей», наступившей индустрии 4.0. Насколько готово российской общество к таким переменам, и как быстро смогут государственные и муниципальные информационные системы адаптироваться под новые требования?

Все новейшие реформации относительно информационных систем направлены на приведение в цифровой вид и объединение существующих данных. Например, согласно заявлению представителей Министерства связи и массовых коммуникации Российской Федерации, в будущем возможно появление единой платформы, которая позволит объединить услуги, предоставляемые органами государственной власти [1]. Причиной этому является многообразие интерфейсов порталов информационных систем каждого государственного органа, отсутствие единой концепции и политики в сфере оказания электронных услуг. Если перейти на предыдущий уровень организации оказания электронных услуг, а именно – на создание и использование информационных систем, то необходимо отметить, что каждая из информационных систем имеет определенные этапы развития, схожие для всего множества таких объектов информационной сферы. Необходимо отметить, что существование единой концепции на этапе создания и развития информационных систем могло бы способствовать наименее безболезненной консолидации существующих ресурсов.

В случае рассмотрения одного объекта из множества информационных систем, можно заметить, что информационные системы, подобно объектам живого мира, проходят различные этапы в течение всего периода их существования – от создания до завершения использования. Для верного в юридическом смысле физического использования пула информационных систем необходимо иметь четко определенные характеристики каждого из этапов жизненного цикла информационных систем. К сожалению, в отечественном законодательстве отсутствует нормативный правовой акт, который бы позволял дифференцировать информационные потоки в различные периоды жизненного цикла информационной системы. Несмотря на доработанное постановление Правительства № 676 [2], вопросы, связанные с объединением и завершением использования информационных систем, остались без должного внимания. По мнению автора, именно жестко установленные границы, определенные субъектный состав и набор правоотношений между субъектами в дальнейшем позволят избежать коллизии при необходимости объединять или актуализировать информационные системы.

Укрупняя все этапы жизненного цикла информационных систем, которые определены в государственном стандарте – документе, имеющем методическую ценность, но не юридическую силу, можно определить стадию создания, использования и вывода из эксплуатации. Наиболее проработанной стадией является стадия использования, поскольку она представляет собой рутинные процессы ввода и обработки информации, в ходе которых должны сохраняться основные критерии информационной безопасности [3] – целостность, доступность и конфиденциальность информации. К слову сказать, обновление или модернизация уже эксплуатируемой информационной системы, или ее сегмента, возвращает информационную систему на этап ее создания. Именно на начальных этапах необходимо закреплять правовое нормы, согласно которым будет происходить регламентирование отношений, возникающих при создании, введение в эксплуатацию, модернизации информационной системы. Такие требования должны быть систематизированы и конкретизированы, что позволит избежать последующих проблем при консолидации с другими информационными системами или при поглощении информационной системы.

Использование информационных систем должно происходить с учетом требований соответствия информационной системе текущей модели угроз; в случае возникновения угроз и невозможности устранить такие угрозы, необходимо прекращать использование информационной системы до устранения последствий реализации угрозы. Кроме этого,

возможно проектировать и внедрять систему мониторинга обеспеченности ресурсами информационной системы, где на основании показателей определенных параметров будет произведен анализ наличия реализации угроз информационной системы.

Кроме этого, необходимо разделять меры по возобновлению работы информационной системы в зависимости от правового режима информации, которая обрабатывается и хранится в информационной системе. Например, утечка обезличенных персональных данных, очевидно, причинит меньший вред, нежели утечка необезличенных персональных данных.

Возвращаясь к вопросу о единообразии при создании и проектировании информационных систем, необходимо также отметить, что важно указать алгоритм вывода информационной системы из эксплуатации и последующего хранения информации, если это необходимо в силу требований законодательства. Так, необходимо предусмотреть возможность использования или возобновления обработки обезличенных персональных данных, или, например, биометрических персональных данных, последующее использование которых возможно только при наличии специального технического либо программного обеспечения.

Одним из немаловажных факторов, обеспечивающих бесперебойное использование информационной системы является организационный фактор. Сотрудники органов государственной власти и органов местного самоуправления работают как с внутренней частью информационной системы – обеспечивая ее технологическую исправность, так и с внешней – работая в качестве операторов или посредников между системой и пользователями информационных систем (например, гражданами в случае оказания услуг населению). В немногочисленных нормативных актах, регламентирующих отношения, возникающие при использовании информационных систем, не указан перечень мероприятий по подготовке сотрудников органов государственной власти и местного самоуправления к работе с информационной системой.

Учитывая последние тенденции в развитии информационных технологий, которые отражены в Стратегии развития информационного общества в Российской Федерации [4], государственной программе «Цифровая экономика» [5] следует отметить, что в ближайшем будущем органы государственной власти и местного самоуправления все больше будут использовать облачные технологии, которые имеют несколько иную организацию становления и развития, нежели «традиционные» информационные системы. С одной стороны, эксплуатация информационных систем с использованием облачных технологий обходится дешевле, но, с другой стороны, обеспечение защиты информации при использовании облачных и иных распределенных технологий требует большее количество финансовых вложений. Чтобы процесс перехода от информационных систем к облачным сервисам был наименее болезненным, необходимо понимать, что только четка структура и понимание всех этапов жизненного цикла информационных систем позволит провести такие изменения.

Литература

1. Все государственные сайты и сервисы объединят на единой платформе [Электронный ресурс]. Режим доступа: URL: http://gov.cnews.ru/news/top/2017-12-13_vse_gosudarstvennye_sajty_i_servisy_obedinyat (дата обращения 19.12.2017)

2. О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации. Постановление Правительства РФ от 06.07.2015 № 676[Электронный ресурс]. Режим доступа: URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102375086&rdk=&backlink=1 (дата обращения 19.12.2017)

3. См., например: ГОСТ 34.601-90 Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания; ГОСТ Р ИСО/МЭК 15026-1-2016 Системная и программная инженерия. Гарантирование систем и программного обеспечения; ГОСТ Р 56713-2015 (ISO/IEC/IEEE 15289:2011) Системная и программная инженерия. Содержание информационных продуктов процесса жизненного цикла систем и программного обеспечения и т.д.

4. Указ Президента Российской Федерации от 09.05.2017 г. № 203 О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы [Электронный ресурс]. Режим доступа: СПС КонсультантПлюс

5. Распоряжение Правительства Российской Федерации от 28.07.2017 г. № 1632-р [Электронный ресурс]. Режим доступа: URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения 19.12.2017)

References

1. Vse gosudarstvennye sajty i servisy ob#edinjat na edinoj platforme [Jelektronnyj resurs]. Rezhim dostupa: URL: http://gov.cnews.ru/news/top/2017-12-13_vse_gosudarstvennye_sajty_i_servisy_obedinyat (data obrashhenija 19.12.2017)

2. O trebovanijah k porjadku sozdanija, razvitija, vvoda v jekspluataciju, jekspluatacii i vyvoda iz jekspluatacii gosudarstvennyh informaci-onnyh sistem, i dal'nejshego hranenija soderzhashhejsja v ih bazah dan-nyh informacii. Postanovlenie Pravitel'stva RF ot 06.07.2015 № 676[Jelektronnyj resurs]. Rezhim dostupa: URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd= 102375086&rdk=&backlink=1 (data obrashhenija 19.12.2017)

3. Sm., naprimer: GOST 34.601-90 Mezhgosudarstvennyj standart. In-formacionnaja tehnologija. Kompleks standartov na avtomatizirovan-nye sistemy. Avtomatizirovannye sistemy. Stadii sozdanija; GOST R ISO/MJeK 15026-1-2016 Sistemnaja i programmnaja inzhenerija. Garan-tirovanie sistem i programmnogo obespechenija; GOST R 56713-2015 (ISO/IEC/IEEE 15289:2011) Sistemnaja i programmnaja inzhenerija. So-derzhanie informacionnyh produktov processa zhiznennogo cikla si-stem i programmnogo obespechenija i t.d.

4. Ukaz Prezidenta Rossijskoj Federacii ot 09.05.2017 g. № 203 O Strategii razvitija informacionnogo obshhestva v Rossijskoj Fede-racii na 2017 – 2030 gody [Jelektronnyj resurs]. Rezhim dostupa: SPS Konsul'tant+

5. Rasporjazhenie Pravitel'stva Rossijskoj Federacii ot 28.07.2017 g. № 1632-r [Jelektronnyj resurs]. Rezhim dostupa: URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (data obrashhenija 19.12.2017) Vse gosudarstvennye sajty i servisy ob#edinjat na edinoj platforme http://gov.cnews.ru/news/top/2017-12-13_vse_gosudarstvennye_sajty_i_servisy_obedinyat

---

Чубукова Светлана Георгиевна, кандидат юридических наук., доцент кафедры правовой информатики Московского государственного юридического университета имени О.Е. Кутафина. 123001, г. Москва, улица Садовая-Кудринская, 9.

CHUBUKOVA Svetlana, candidate of law science, associate professor at Kutafin Moscow State Law University. Sadovaya – Kudrinskaya Ulitsa, 9, Moskva, 123001

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ

Объем статьи не должен превышать 40 тыс. знаков, включая пробелы, и не может быть меньше 5 страниц. Статья набирается в текстовом редакторе Microsoft Word в формате *.rtf шрифтом Times New Roman, размером 14 пунктов, в полуторном интервале. Отступ красной строки: в тексте — 10 мм, в затекстовых примечаниях (концевых сносках) отступы и выступы строк не ставятся. Точное количество знаков можно определить через меню текстового редактора Microsoft Word (Сервис — Статистика — Учитывать все сноски).

Параметры документа: верхнее и нижнее поле — 20 мм, правое — 15 мм, левое — 30 мм.

В начале статьи помещаются: инициалы и фамилия автора (авторов), название статьи, **аннотация** на русском языке объемом **не менее 700 знаков или 10 строк,** ниже отдельной строкой — ключевые слова. **Ключевые слова** приводятся в именительном падеже в количестве до десяти слов. Инициалы и фамилия автора (авторов) дублируются транслитерацией. **Должны быть переведены на английский язык название статьи, аннотация, ключевые слова.**

УДК
ББК

ОБРАЗЕЦ

А. А. Первый, Б. Б. Второй, В. В. Третий

НАЗВАНИЕ СТАТЬИ, ОТРАЖАЮЩЕЕ ЕЕ НАУЧНОЕ СОДЕРЖАНИЕ, ДЛИНОЙ НЕ БОЛЕЕ 12—15 СЛОВ

Аннотация набирается одним абзацем, отражает научное содержание статьи, содержит сведения о решаемой задаче, методах решения, результатах и выводах. Аннотация не содержит ссылок на рисунки, формулы, литературу и источники финансирования. Рекомендуемый объем аннотации — около 50 слов, максимальный — не более 500 знаков (включая пробелы).

Ключевые слова: список из нескольких ключевых слов или словосочетаний, которые характеризуют Вашу работу.

Рисунки

Вставляются в документ целиком (не ссылки). Рекомендуются черно-белые рисунки с разрешением от 300 до 600 dpi. Подрисуночная подпись формируется как надпись («Вставка», затем «Надпись», без линий и заливки). Надпись и рисунок затем группируются, и устанавливается режим обтекания объекта «вокруг рамки». Размер надписей на рисунках и размер подрисуночных подписей должен соответствовать шрифту Times New Roman, 8 pt, полужирный. Точка в конце подрисуночной подписи не ставится. На все рисунки в тексте должны быть ссылки.

Все разделительные линии, указатели, оси и линии на графиках и рисунках должны иметь толщину не менее 0,5 pt и черный цвет. Эти рекомендации касаются всех графических объектов и объясняются ограниченной разрешающей способностью печатного оборудования.

Формулы

Набираются со следующими установками: стиль математический (цифры, функции и текст — прямой шрифт, переменные — курсив), основной шрифт — Times New Roman 11 pt, показатели степени 71 % и 58 %. Выключенные формулы должны быть выровнены по центру. Формулы, на которые есть ссылка в тексте, необходимо пронумеровать (сплошная нумерация). Расшифровка обозначений, принятых в формуле, производится в порядке их использования в формуле. Использование букв кириллицы в формулах не рекомендуется.

Таблицы

Создавайте таблицы, используя возможности редактора MS Word или Excel. Над таблицей пишется слово «Таблица», Times New Roman, 10 pt, полужирный, затем пробел и ее номер, выравнивание по правому краю таблицы. Далее без абзацного отступа следует таблица. На все таблицы в тексте должны быть ссылки (например, табл. 1).

Примечания

Источники располагаются в порядке цитирования и оформляются по ГОСТ 7.05-2008.

Статья публикуется впервые
Подпись, дата

В конце статьи перед данными об авторе должна быть надпись *«Статья публикуется впервые»,* ставится дата и авторучкой подпись автора (авторов). При пересылке статьи электронной почтой подпись автора сканируется в черно-белом режиме, сохраняется в формате *.tif или *.jpg и вставляется в документ ниже затекстовых сносок. (Либо сканируется последняя страница статьи с подписью и высылается по электронной почте отдельным файлом.)

Обязательно для заполнения: в конце статьи (в одном файле) на русском языке помещаются сведения об авторе (авторах) — полностью имя, отчество, фамилия, затем ученая степень, ученое звание, должность, кафедра, вуз (или организация, в которой работает автор); рабочий адрес вуза или организации (полные – включая название, город и страну – адресные сведения вместе с почтовым индексом, указывать правильное полное название организации, желательно – его официально принятый английский вариант), электронный адрес и контактные телефоны. **Эти данные об авторе должны быть переведены на английский язык.**

Для рассмотрения вопроса о публикации статьи в редакцию журнала необходимо выслать на электронную почту:

1) рукопись статьи, подписанную на последней странице всеми авторами. В рукописи должны быть полные сведения об авторах;

2) в случае, если статья имеет рецензию и заверена печатью, ее оригинал необходимо отправить в редакцию и по электронной почте в отсканированном виде с обязательным указанием контактов рецензента;

3) на статью необходимо выслать экспертное заключение о возможности открытого опубликования (образцы: заключение от руководителя эксперта или заключение от экспертной комиссии.

Библиографические ссылки

Цитируемая в статье литература приводится в виде списка в конце текста. В тексте в квадратных скобках дается ссылка на порядковый номер списка (ГОСТ Р 7.0.5.-2008). Полный текст ГОСТа размещен на официальном сайте Федерального агентства по техническому регулированию и метрологии Авторские примечания (не являющиеся используемой литературой или ссылкой на источник) размещаются в постраничных сносках.

Ниже приводятся образцы оформления сносок:

а) на монографии:

[1] Белова М. С., Кинсбурская В. А., Ялбулганова А. А. Налоговый контроль и ответственность: анализ законодательства, административной и судебной практики / под ред. А. А. Ялбулганова.— М. : Знание, 2008.— С. 12.

б) на статьи из сборников:

[1] Клишина М. А. Новое в порядке составления проекта бюджета // Финансовое право России: актуальные проблемы / под ред. А. А. Ялбулганова.— М., 2007.— С. 101.

в) статьи из журналов и продолжающихся изданий:

[1] Глушко Е. К. Административно-правовая природа государственных корпораций // Реформы и право.— 2008.— № 3.— С. 38—43.

г) авторефераты диссертаций:

[1] Стрижова О. А. Правовое регулирование таможенной стоимости : автореф. дис. … канд. юрид. наук.— М., 2008.— С. 7.

д) интернет-страницы:

Противодействие коррупционным правонарушениям // Юридическая Россия: федеральный правовой портал. URL: http://law.edu.ru/news/news.asp?newsID=12954 (дата обращения: 08.01.2009).

В редакцию журнала статья передается качественно по электронной почте одним файлом (название файла — фамилия автора). Тема электронного письма: Вестник УрФО. Безопасность в информационной сфере.

Отправляемая статья должна быть вычитана автором; устранены все грамматические, пунктуационные, синтаксические ошибки, неточности; выверены все юридические и научные термины. За ошибки и неточности научного и фактического характера ответственность несет автор (авторы) статьи.

Поступившие в редакцию материалы возврату не подлежат.

Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru
в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».

Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76,
ЮУрГУ, Издательский центр.

ВЕСТНИК УрФО
Безопасность в информационной сфере № 4(26) / 2017

Дата выхода в свет 29.12.2017. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 5,25. Тираж 100 экз. Заказ 386/638.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 4(26) / 2017

Date of publication of the 29.12.2017. Format 70×108 1/16. Screen printing.
Conventional printed sheet 5,25. Circulation – 100 issues. Order 386/638. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080