ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 1(23) / 2017

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+

В НОМЕРЕ

IN THIS ISSUE

Вестник УрФО № 1(23) / 2017, с. 4–9
УДК 004.056.53 + 336.717.111.7:004.738.5.056

Григоров А. С.

ИСПОЛЬЗОВАНИЕ АНАЛИЗА SQL-ЗАПРОСОВ ДЛЯ ОБНАРУЖЕНИЯ АТАК НА СИСТЕМЫ МОБИЛЬНОГО БАНКИНГА

В данной статье рассмотрены основные типы уязвимостей приложений мобильного банкинга и возможные атаки в разрезе функциональности приложений и типов интеграционных сервисов на стороне серверного ПО систем мобильного банкинга. Предложен метод обнаружения некоторых уязвимостей на основе анализа SQL-запросов, выполняемых к СУБД системы дистанционного банковского обслуживания (ДБО), дающий дополнительные возможности качественно снизить количество ложноположительных и ложноотрицательных ошибок обнаружения мошеннических операций в системах ДБО. Даны рекомендации по организации процесса разработки систем мобильного банкинга, позволяющие снизить риск возникновения уязвимостей в создаваемых системах.

Ключевые слова: *мобильный банкинг, системы противодействия мошенничеству, обнаружение аномалий, SQL, СУБД.*

Grigorov A. S.

USING THE ANALYSIS OF SQL-QUERIES TO DETECT ATTACKS ON MOBILE BANKING SYSTEM

This paper describes the main types of mobile banking application vulnerabilities and possible attacks in the context of the functionality of applications and types of integration services on the side of the server software of mobile banking system. Propose the method for detecting certain vulnerabilities by analyzing the SQL-queries performed to the database of e-banking system (RBS), which gives additional opportunities to reduce false positives and false negative error detection of fraudulent transactions in RBS systems. This paper also provides recommendations of the organization of the development process of mobile banking systems that reduce the risk of vulnerabilities in established systems.

Keywords: *mobile banking, anti-fraud system, anomaly detection, SQL, RDBMS.*

Согласно результатам исследования[1], проведённого «Markswebb Rank & Report» в ноябре-декабре 2015 года, мобильными банковскими приложениями для смартфонов и планшетов в Российской Федерации пользуются 18,1 млн. человек, что составляет 33% российской интернет-аудитории. В 2014 году оборот на российском рынке мобильного банкинга составил 15 млрд. рублей[8], при этом по прогнозам «J'son & Partners Consulting» среднегодовой темп роста с 2014 по 2018 года составит 28%. В тоже время результат анализа мобильных приложений российских банков[7] показывает, что разработчики мобильных приложений не уделяют должного внимания вопросам безопасности и не следуют рекомендациям по безопасной разработке под конкретные мобильные операционные системы. При этом стоит отметить, что список уязвимостей приложений мобильного банкинга во многом схож со списком уязвимостей мобильных приложений в целом[7], представленным в отчёте OWASP Top 10 Mobile Risks 20143. Это позволяет говорить о потенциальной возможности выполнения широко распространённых атак на мобильные банковские приложения без знания специфики их работы, что снижает требования к навыкам злоумышленников для осуществления успешной атаки.

В данной статье будут рассмотрены основные типы уязвимостей приложений мобильного банкинга и представлена карта возможных атак в разрезе функциональности приложений и типов интеграционных сервисов на стороне серверного ПО систем мобильного банкинга. Также будет предложен метод обнаружения некоторых уязвимостей на основе анализа SQL-запросов, выполняемых к СУБД системы дистанционного банковского обслуживания (ДБО).

Организация серверной части системы мобильного-банкинга

В настоящий момент возможности мобильных операционных систем не ограничивают разработчиков, позволяя создавать сервисы, не уступающие по функциональности традиционным интернет-банкам. Если ранее банки через мобильные приложения предоставляли в первую очередь информационные сервисы, такие как просмотр списка счётов, получение информации о проведённых транзакциях или просмотр остатка на карточном счёте, то сейчас ситуация существенно изменилась. Преследуя цели сокращения операционных издержек, расширения клиентской базы и увеличения комиссионных доходов, банки стремятся нарастить функциональные возможности дистанционных сервисов, в частности добавляя возможность выполнения платежных операций, P2P-переводов, операций онлайн-кредитования. Однако, помимо удобства для клиентов банка, возрастает угроза кражи денежных средств.

Типичным вариантом организации работы приложений мобильного банкинга является подход, когда на стороне сервера ДБО определяется набор сервисов, к которым приложение мобильного банка выполняет обращение через интернет. Взаимодействие между мобильным приложением и сервером может быть построено на основе RESTful веб-сервисов, протокола SOAP или других подходов, работающих поверх HTTP. Мобильное приложение выступает инициатором взаимодействия, отправляя запрос, а сервер системы ДБО выполняет запрашиваемое действие и возвращает ответ. В зависимости от используемой технологий, форматы передачи данных запросов и ответов могут быть разными, наиболее распространенными являются XML и JSON.

Набор прикладных сервисов и операций, которые входят в API системы ДБО для мобильных платформ, зависит о специфики конкретных систем и функциональности разрабатываемых мобильных приложений. Типовой набор бизнес операций, доступный в приложениях мобильного банкинга для физических лиц от ведущих российских компаний разработчиков систем ДБО, можно по функциональному назначению разделить на несколько групп[2,10]:

1. Сервисы авторизации и безопасности:

– аутентификация клиента по логину и паролю;

– завершение текущей сессии;

– смена пароля для доступа к системе ДБО;

– регистрация мобильного устройства, привязка устройства к учётной записи клиента банка;

– получение паролей 3-D Secure;

– выполнение подтверждения корректности введённых реквизитов платежных распоряжений и заявок.

2. Информационные сервисы:

– получение списков текущих счетов,

карт, вкладов, кредитов, металлических счётов, а также их основных атрибутов (номера счетов, остатки на счетах, тарифные планы);

– получение реквизитов пополнения текущих, карточных, депозитных счетов, а также реквизитов для погашения кредита;

– получение графика платежей по кредиту;

– получение выписок по счетам и списков последних транзакций по карте (включая находящихся на исполнении), анализ расходов;

– получение реквизитов виртуальных карт (номер карты, имя владельца, срок действия карты, CVV2/CVC2);

– получение информации об истории операций, выполненных в разных каналах системы ДБО;

– получение анкетных данных клиента для отображения в интерфейсе приложения (ФИО; название отделения банка, в котором обслуживается клиент; номер документа, удостоверяющего личность; ИНН; номера мобильных телефонов и email'ов);

– получение новостной ленты банка, информации о курсах конвертации валют, рекламных предложений, списка банкоматов и офисов банка.

3. Платёжные сервисы:

– выполнение переводов между счетами и картами клиента;

– выполнение внешних переводов по свободным реквизитам, оплата налогов и выполнение платежей в бюджет;

– переводы по номеру карты;

– получение информации о начислениях через систему ГИС ГМП по паспортным данным или ИНН пользователя или уникальному идентификатору начисления;

– оплата услуг, согласно каталогу поставщиков услуг;

– получение списка шаблонов платежей и их выполнение.

4. Сервисы подачи заявок:

– заявки на открытие и закрытие текущих счётов и вкладов;

– заявки на выпуск, блокировку карт (в том числе виртуальных).

Типовые уязвимости систем мобильного банкинга

Атаки на мобильное приложение могут быть выполнены:

– через вредоносное приложение, установленное на том же устройстве, что и приложение мобильного банка;

– путем модификации кода мобильного приложения;

– при наличии контроля канала связи (атака «человек посередине»).

Так согласно исследованию компании Digital Security[7], проведённому в 2013 году, 35% рассмотренных приложений мобильного банкинга, написанных под операционную систему iOS, некорректно организовывали работу с SSL (например, не выполнялась проверка SSL-сертификата банка), что позволяло выполнять перехват и подмену передаваемых данных между приложением и серверной частью. Подмена значений параметров запросов наиболее опасна, так как может привести к исполнению банковских операций с реквизитами, желаемыми злоумышленниками.

Техника защиты серверной части мобильного банка схожа с защитой серверов интернет-банков. Так при разработке серверной части мобильного банкинга следует исходить из того, что любым данным, передаваемым в запросах, нельзя доверять, так как они могут быть подменены злоумышленником. Следовательно, все входные данные должны проходить предварительную проверку. Однако на практике невыполнение или неполное выполнение этих требований не является редкостью: 18% систем ДБО, исследованных компанией Positive Technologies[9], имели уязвимость к SQL-инъекциям. В то же время атаки могут быть выполнены и без применения сложных техник. В случае если на стороне серверной части не выполняется должная проверка связи текущей сессии пользователя с данными, которые передаются в запросе, то, подменив параметры запроса (например, идентификатор счёта назначения перевода), злоумышленник может инициировать выполнение операции, недопустимой с точки зрения бизнес-процессов, заложенных в систему ДБО.

Наличие подобных ошибок в реализации сервисов, относящихся к группе информационных сервисов, а также сервисов получения паролей 3-D Secure, получения списка начислений из ГИС ГМП и получения списков шаблонов платежей может привести к нарушению конфиденциальности данных системы ДБО. В то же время недостаточная обработка входных данных для сервисов из групп «сервисы авторизации и безопасности», «платежные сервисы» и «сервисы подачи заявок» может привести к атакам на целостность и до-

ступность данных в информационных системах банка.

Стоит отметить, что причиной подобных ошибок может являться отсутствие упоминания необходимости проверки входных данных сервисов в функциональных требованиях и технических заданиях на разработку систем. Это приводит к тому, что разработчики не реализуют обработку входных данных, так как это явно не указано в техническом задании, а при функциональном тестировании не рассматриваются сценарии выполнения нелегитимных запросов. Как следствие, существующая уязвимость на этапе тестирования не обнаруживается, и разработанная система запускается в промышленное использование вместе с ней. В качестве возможной меры по уклонению от подобных рисков может являться обязательное выполнение тестирования на проникновение перед запуском системы в промышленное использование, а также использование специализированных систем обнаружения мошеннических операций, которые выполняют анализ операций, проводимых в системах ДБО.

Обнаружения вторжений и мошеннических операций в системах ДБО

На рисунке 1 приведена схема организации работы системы ДБО совместно с системой обнаружения вторжений и мошеннических операций. Принцип работы системы обнаружения вторжений (СОВ) заключается в том, что СОВ анализирует события, происходящие в банковских системах, и в случае обнаружения отклонения работы этих систем от предопределённых шаблонов нормального поведения выполняет информирование специалистов службы безопасности банка (через e-mail, SMS, административную консоль СОВ) или осуществляет активные действия по предотвращению выполнения операции (например, выполняется блокировка учётной записи пользователя или отказ в выполнении операции).

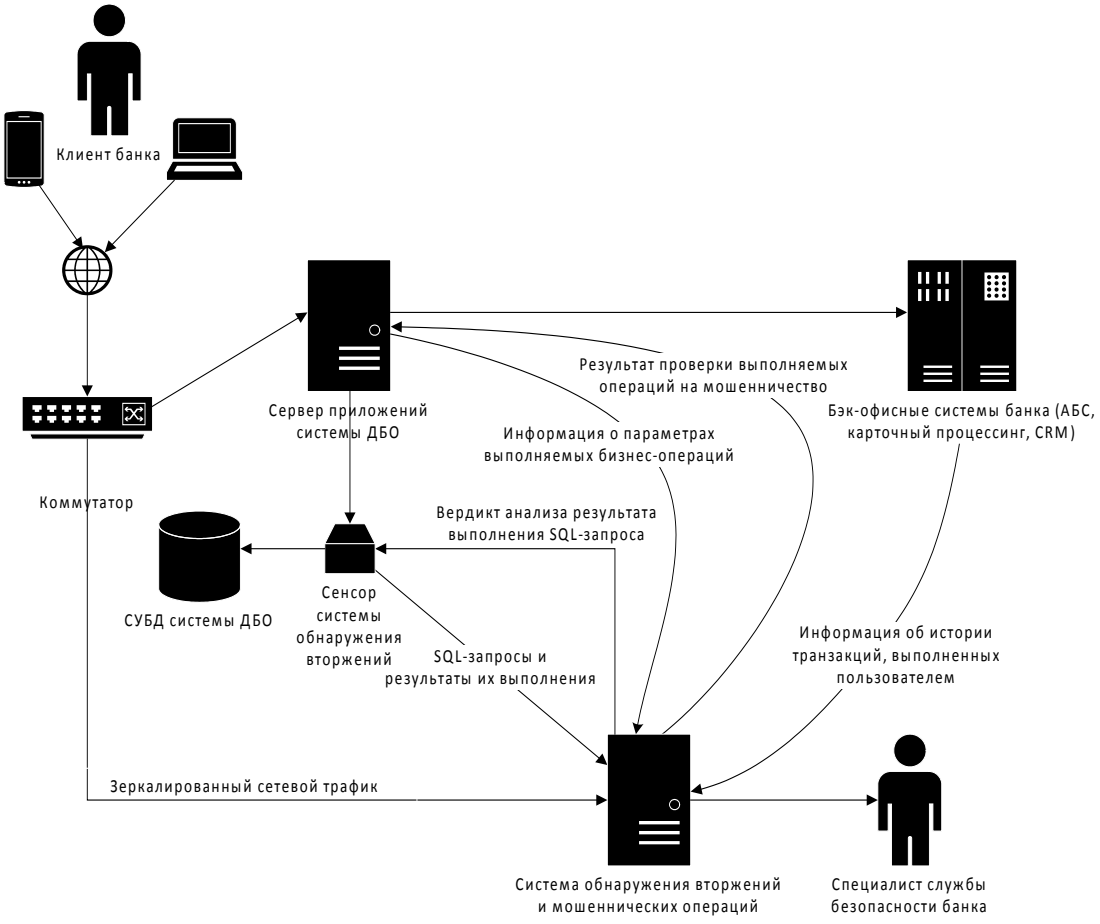


Рис. 1 Схема организации обнаружения мошеннических операций в действиях пользователей системы ДБО

Современные СОВ для анализа событий, происходящих в защищаемой информационной системе, могут агрегировать данные из различных источников. Например, СОВ может анализировать зеркалированный сетевой трафик, идущий к серверам системы ДБО. Однако разработка правил проверки сетевого трафика может потребовать высоких временных и финансовых затрат, связанных с выполнением реверс-инжиниринга используемых протоколов. Для выполнения более качественного анализа современные СОВ могут обмениваться с системой ДБО сообщениями, содержащими информацию о параметрах выполняемых бизнес-операций. Так, например, система ДБО может передать СОВ информацию о реквизитах платежа, IP-адресе и IMEI смартфона, с которого выполняется платёж. СОВ же в свою очередь выполняет проверку переданных данных по набору правил и алгоритмов и выставляет итоговую оценку, на основе которой принимается решение, аномальна ли выполняемая операция или типична для данного пользователя. Организация такого взаимодействия между системой ДБО и СОВ требует специальной доработки системы ДБО, что влечёт за собой дополнительные затраты.

Так как большинство систем ДБО используют для хранения данных реляционные СУБД, а основным средством коммуникации являются SQL-запросы, то альтернативным вариантом можно предложить использовать для получения дополнительных данных о семантике выполняемых пользователем операций анализ выполняемых SQL-запросов и получаемых результатов. При этом, используя подход экранирования драйверов БД[6], можно организовать интеграцию СОВ и защищаемой информационной системы (ИС) без необходимости выполнения доработок на стороне ИС и СУБД.

Автором данной статьи разработан метод обнаружения аномального поведения пользователей ИС на основе оценки результата выполнения SQL-запросов, которые ИС инициировала к СУБД, обрабатывая команды от пользователя[5]. Принятие решения о допустимости выполняемой операции осуществляется путём сравнения полученной выборки данных с ожидаемым результатом, который соответствует профилю нормального поведения пользователя базы данных. Профиль представляет собой граф, отражающий взаимосвязи между данными, которые выбираются SQL-запросами, считающимися допустимыми для нормальной работы пользователя. Использование данного подхода позволяет обнаруживать как атаки на основе SQL-инъекций, так и попытки эксплуатации возможных уязвимостей, связанных с недостаточной проверкой разграничения прав доступа в прикладном коде информационной системы[4].

Метод обнаружения аномального поведения пользователя на основе оценки результатов выполнения SQL-запросов может использоваться для обнаружения атак на сервисы системы ДБО, реализация бизнес-логики которых подразумевает обращение к БД за данными с использованием значений параметров вызова сервисов в качестве аргументов условий SQL-выражений. К таким сервисам, в частности, относятся сервисы выполнения платежей и переводов, получения паролей 3-D Secure и реквизитов виртуальных карт, сервисы получения информации по банковским продуктам клиента, сервисы подачи заявок на открытие или закрытие вклада, выпуск карты.

Рассмотрим, например, сервис открытия вклада, который в качестве входных параметров получает идентификатор счёта клиента, с которого будет выполнен перевод начальной суммы вклада, значение начальной суммы, идентификатор связанного счёта для выплаты процентов и другие параметры открываемого вклада. Злоумышленник может предпринять атаку, пытаясь, например, подменить идентификатор счёта списания на идентификатор счёта, принадлежащего другому клиенту, для того чтобы открыть вклад за счёт средств другого клиента. Или же, наоборот, выполняя атаку «человек посредине», злоумышленник может осуществить подмену идентификатора счёта зачисления процентов для того, чтобы впоследствии проценты по вкладу переводились на нужный ему счёт. При обработке вызова сервиса система ДБО выполняет запрос к БД на получение информации о требующихся счетах. Запрос может иметь следующий вид:

select * from accounts where id in (123, 456);

Согласно разработанному методу[5] данным, полученным в результате выполнения запроса, ставится в соответствие граф, отражающий взаимосвязи между данными попавшими в результат выборки с учётом информации о том, от имени какого пользователя выполнялся запрос. Так каждой записи соответ-

ствует вершина в графе, а вес ребра между двумя вершинами графа равен вероятностьи совместного появления соответствующих записей в результате выполнения SQL-запросов, характерных для нормального поведения пользователя. В дальнейшем на основе рассчитанных характеристик графа, таких как модульность или плотность рёбер, принимается решение о признании результата ожидаемым или аномальным.

Заключение

Ежегодный рост количества пользователей дистанционных сервисов банка, в частности сервисов мобильного банкинга, ставит перед банками новые задачи по обеспечению безопасности использования предоставляемых сервисов. Один из эшелонов защиты систем ДБО – системы обнаружения вторжений и мошеннических операций. В данной статье был предложен вариант использования анализа SQL-запросов, выполняемых системой ДБО, в качестве дополнительного источника информации для принятия решения о подозрительности выполняемых операций. Как следствие, появляются дополнительные возможности качественно снизить количество ложноположительных и ложноотрицательных ошибок обнаружения мошеннических операций.

Примечания

1. e-Finance User Index 2016. [Электронный ресурс]. Режим доступа: http://markswebb.ru/e-finance/e-finance-user-index-2016/. Дата обращения: 13.03.2016.

2. InterBank Mobile Retail // R-Style Softlab: сайт [Электронный ресурс]. Режим доступа: http://softlab.ru/solutions/interbank/5224/

3. Top 10 Mobile Risks. [Электронный ресурс]. Режим доступа: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks. Дата обращения: 13.03.2016.

4. Беляев А.В. Обнаружение атак на базы данных на основе оценки внутренней структуры результатов выполнения SQL-запросов. / А.В. Беляев, А.С. Григоров // Научно-технический вестник Поволжья. №2 2012 г. - Казань: Научно-технический вестник Поволжья, 2012. – С. 99-104.

5. Григоров А.С., Плашенков В.В. Метод обнаружения аномалий в поведении пользователей на основе оценки результатов выполнения SQL-запросов / А.С. Григоров, В.В. Плашенков // Вестник компьютерных и информационных технологий. – 2013. – №3 – С. 49-54.

6. Григоров А.С. О способе интеграции системы обнаружения аномалий в SQL запросах к базе данных на основе результатов выполнения запроса с приложениями, использующими СУБД в качестве хранилища данных [Текст] / А.С. Григоров // Молодой ученый. — 2011. — №12. Т.1. — С. 21-24.

7. Миноженко А. Безопасность мобильных банковских приложений. / А. Миноженко // Information Security / Информационная безопасность. №4, 2013 – с. 30-32.

8. Мобильный банкинг в РФ: прогнозы рынка, поведение пользователей, рейтинг приложений. [Электронный ресурс]. Режим доступа: http://json.tv/ict_telecom_analytics_view/mobilnyy-banking-v-rf-prognozy-rynka-povedenie-polzovateley-reyting-prilojeniy-20150525095123. Дата обращения: 13.03.2016.

9. Статистика уязвимостей систем дистанционного банковского обслуживания (2011-2012). [Электронный ресурс]. Режим доступа: http://www.ptsecurity.ru/download/Analitika_DBO.pdf. Дата обращения: 05.04.2016.

10. Универсальный мобильный клиент. // Компания БСС: сайт [Электронный ресурс]. Режим доступа: http://www.bssys.com/solutions/financial-institutions/dbo-bs-client-chastnyy-klient/chk-mobilnyy-klient/

ГРИГОРОВ Андрей Сергеевич, старший преподаватель, кафедра инфокоммуникационных технологий и безопасности, ФГБОУ ВПО «Череповецкий государственный университет». 162602, г. Череповец, Советский пр-т, д. 8. E-mail: andreygrigorov1986@gmail.com

GRIGOROV Andrey, is a senior lecturer, Department of Information and Communication Technology and Security, Federal State Budget Educational Institution of Higher Education «Cherepovets State University». 162602, Cherepovets, Sovetsky ave., h.8. E-mail: andreygrigorov1986@gmail.com

УДК - 004.056.53 + 658:004.4.056 + 004.738.5.056 Вестник УрФО № 1(23) / 2017, с. 10–13

Гузенкова Е. А.

ПРИМЕНЕНИЕ СРЕДСТВ ЗАЩИТЫ ПРИ ВЗАИМОДЕЙСТВИИ МОБИЛЬНЫХ УСТРОЙСТВ С КОРПОРАТИВНОЙ СРЕДОЙ ПРЕДПРИЯТИЯ

В статье проводиться анализ вопросов безопасности при использовании мобильного устройства в качестве средства, входящего в состав информационной системы на предприятиях, с помощью которого осуществляется взаимодействие с корпоративной средой предприятия. Рассматриваются вопросы организации доступа мобильных устройств в корпоративную сеть предприятия посредством сети передачи данных с использованием средств шифрования. Даются рекомендации по комплексному обеспечению безопасности информации при использовании мобильных устройств, как часть программно-аппаратного комплекса информационной системы предприятия, что в свою очередь приведет к повышению мобильности сотрудников предприятия, и позволит им в рамках своих должностных обязанностей иметь доступ через мобильные рабочие места к корпоративным информационным системам.

Ключевые слова: *мобильное устройство, защита информации, программное обеспечение, программно-аппаратный комплекс, передача информации.*

Guzenkova E. A.

THE APPLICATION OF THE REMEDIES IN THE INTERACTION OF MOBILE DEVICES WITH CORPORATE ENTERPRISE ENVIRONMENT

The article analyzes security issues when using mobile devices as a tool that is part of the information system in enterprises, which interacts with corporate enterprise environment. The arrangement of mobile access in the enterprise network through a data transmission network using encryption. Recommendations for integrated information security when using mobile devices as part of hardware-software complex of the enterprise information system, which in turn will lead to increased mobility of employees, and allow them as part of their official duties have access via mobile jobs to corporate information systems.

Keywords: *mobile device, data protection, software, hardware-software complex, the transmission of information.*

Распространение информационных технологий в современном мире привело к тому, что практически на каждом предприятии происходить автоматизация основной и вспомогательной деятельности. Крупные предприятия не ограничиваются локальным сегментом, и с расширением их сфер деятельности происходит их глобализация. Происходит распределение функциональной нагрузки по филиалам предприятия, за счет взаимодействия структурных единиц предприятия посредством распределенной информационной системы или систем. Современные условия рынка заставляют предприятия осваивать также и мобильную площадку взаимодействия своих сотрудников с корпоративной сетью, посредством организации доступа к информационным системам предприятия за счет создания мобильных рабочих мест, в качестве которых рациональнее всего использовать современные мобильные устройства.

Введение в структуру информационного обмена корпоративной сети создает необходимость дополнительной защиты информации при передаче ее между мобильных рабочим местом и корпоративной сетью.

Защита инфраструктуры, включающей в себя мобильные рабочие места предусматривает, как защиту информации, находящейся непосредственно на мобильном устройстве, так и при передаче ее через сеть передачи данных на сервера, обслуживающие информационную систему корпоративной сети.

Как показывает статистика последнего года, при подключении устройства к корпоративной сети утечка информации конфиденциального характера может произойти как на стадии хранения этой информации непосредственно на устройстве, так и при передаче ее через сеть.

При хранении информации непосредственно на устройстве, возникает угроза проникновения троянских программ на устройство, по статистики компании «Лаборатория Касперского» в 2016 году было обнаружено 1520931 вредоносных установочных пакетов мобильных угроз[1]. Основными способами заражения является использование рекламы, установка мобильных приложений (в том числе с официального магазина Google Play Store). Не смотря на постоянные обновления мобильных операционных систем статистический анализ показывает, что злоумышленники научились обходить защитные механизмы, встроенные в мобильные операционные системы. Самыми распространенными результатами вредоносного воздействия является как похищение или искажение конфиденциальной информации, так и создание помех в работе мобильного рабочего места пользователя (например, шифрование данных и попытка вымогательства выкупа, или развертывания активного рабочего окна поверх остальных рабочих столов программой-злоумышленником).

В банке данных угроз Федеральной службы технического и экспортного контроля были зафиксированы 183 уязвимости, имеющие отношение к операционной системе Android, большинство этих уязвимостей относятся к уязвимостям кода, и лишь небольшая часть из них – к уязвимостям архитектуры[2].

Для защиты от несанкционированного доступа к информации, хранящейся и передаваемой между мобильными устройствами и корпоративной сетью необходимо реализовать комплексный характер защиты.

Среди множества представленных на рынке мобильной связи телефонов, большинство используют мобильные телефоны с операционной системой Android. На уровне клиентской мобильной станции аппаратно-программная реализация может быть создана на основе мобильного устройства со встроенными средствами криптографической защиты информации, работа которых необходимо протестировать до введения в эксплуатацию[3]. Преимуществом такой реализации является возможность сертификации устройства на соответствии требованиям регуляторов (ФСБ России).

Другим вариантом решения защищенных мобильных устройств на базе операционной системы Android может стать реализация программно-аппаратного комплекса, заказанного под нужды организации. Таким решением стало устало производство мобильных устройств по заказу ОАО «РЖД», основными компонентами которого являются батарея, камера, тачскрин, контакты, антенны, мембраны влагозащиты, прокладки и наклейки, предназначенные для защиты мобильного устройства от внешних факторов негативного воздействия. Сама операционная система переработала таким образом, в ней устранено большинство уязвимостей, свойственных стандартной операционной системе Android, в том числе уязвимости, связанные с

возможностью предоставления злоумышленникам прав суперпользователя, в том числе в данной операционной системе установлена система защиты от выхода пользователем в сеть Интернет, блокирована возможность замены сим-карты и возможность добавления или удаления приложений, не требующихся для реализации информационного обмена с корпоративной сетью организации[4]. Для осуществления защиты мобильных устройств необходимо использовать защищенную операционную систему, в качестве которой может использоваться специализированная прошивка, разработанная специально под нужды компании, работающая на основе программной платформы с применением квалифицированной электронной подписи (ЭП) компании, посредством которой, мобильное устройство может взаимодействовать с информационными системами предприятия. За счет применения квалифицированной электронной подписи доступ к функционалу операционной системы мобильного устройства может осуществить только тот сотрудник, право доступа которого подтверждается соответствии с сертификатом ЭП подключенной МЭК. Возможность применения квалифицированной ЭП предоставляет возможность создания механизмов разграничения доступа по работе с информацией, которая в последствии будет передаваться в информационную систему предприятия.

В процессе организации безопасной передачи информации между мобильным рабочим местом (мобильным устройством) и корпоративной средой предприятия (информационной системой) необходимо организовать как безопасность самой мобильной станции, так и реализовать виртуальный канал передачи данных[5].

Первую задачу может решить применение специализированной SIM-карты (Subscriber Identity Module), в которой может содержаться информация о сервисах, необходимых для абонента. Предназначение SIM-карты заключается в том, что абонент и само устройство будут однозначно идентифицированы. При этом каждому абоненту будет присвоен уникальный, международный идентификатор мобильного абонента, который состоит из следующих компонентов:

– трехразрядный код страны;

– двухразрядный код сети;

– десятиразрядный код абонента MSIN (Mobile Subscriber Identity Number).

Доступ к SIM-карте защищен PIN-кодом (Personal Identification Number), который осуществляет блокировку карты, при троекратном не правильном вводе данных.

Безопасность информации мобильного устройства обеспечивается шифрованием и уникальным четырнадцатиразрядным идентификатором аппаратуры мобильной связи IMEI (International Mobile Equipment Identity) который позволяет однозначно идентифицировать мобильное устройство. За счет пограничных шлюзов, обеспечивается защита корпоративной сети от вторжений со стороны злоумышленников. В частности, пограничный шлюз защищает оператора от атак, связанных с подменой адреса. Также для обеспечения безопасной передаче информации, на пограничном шлюзе устанавливается соединение VPN между различными операторами[6].

Внутри сети предприятия, для взаимодействия мобильных устройств подключение пользователей организовано посредством корпоративной сети передачи данных, а все мобильные устройства проходят процесс аутентификации в системе Radius по уникальному серийному номеру, что исключает доступ при использовании SIM карт, номера которых не занесены в реестр для доступа в корпоративную сеть. При этом общественные сети не используются, а сетевой трафик от внешнего сетевого интерфейса к информационным ресурсам организации может циркулировать в открытом виде.

Примечания

[1] Унучек Р. Мобильные угрозы // Системный администратор – 2016. – №11 (168). – С. 38-42.

[2] Банк данных угроз информационной безопасности ФСТЭК // Портал ФСТЭКhttp://www.bdu.fstec.ru/vul (дата обращения: 05.05.2017).

[3] Документация АПШК «Континет» // Код безопасностиhttps://www.securitycode.ru/products/apksh_kontinent/documentation/ (дата обращения: 06.05.2017).

[4] Регламент функционирования аккредитованного удостоверяющего центра ОАО «РЖД» утвержденный Директором ГВЦ ОАО «РЖД» 03.032014. – 64 с.

[5] Ожиганова, М.И. Повышение защищенности от несанкционированного доступа компьютерной сети // М.И. Ожиганова, А.В. Колесников, А.Ю. Колодяжная. Новая наука: опыт, традиции, инновации: сборник статей Международной научно-практической конференции (г. Стерлитамак, 24 июня 2015 г.) – Стерлитамак: РИЦ АМИ, 2015. – с. 76 – 78.

[6] Росляков, А.В. Виртуальные частные сети. Основы построения и применения / А.В. Росляков. - М. : Эко-Трендз, 2006. – 304 с.

ГУЗЕНКОВА Елена Алексеевна, старший преподаватель кафедры «Информационные технологии и защита информации», ФГБОУ ВО Уральский государственный университет путей сообщения (УрГУПС), 620032 г. Екатеринбург ул. Колмогорова 66. E-mail: sato-hany@yandex.ru

GUZENKOVA Elena, Senior teacher the Department "Information technologies and protection of information", Ural State University of Railway Transport (USURT). 620032, the city of Ekaterinburg Kolmogorov 66. E-mail: sato-hany@yandex.ru

УДК - 004.056 + 005.334:004.056 Вестник УрФО № 1(23) / 2017, с. 14–19

Баринов А.Е., Рябцева О.В., Соколов А.Н.

АДАПТИВНАЯ ОЦЕНКА КЛИЕНТСКОГО РИСКА В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ

В статье описаны основные угрозы облачных инфраструктур согласно стандарту NIST. Рассмотрена проблема оценки риска для клиента, использующего облачные инфраструктуры. Описаны ранее существующие подходы и стандартные модели. В статье предложено совместное использование статистического подхода и CVSS 3.0 оценок уязвимостей в программных продуктах для расчёта вероятности компрометации облачного сервиса. Использованный подход предполагает проведение отдельных оценок для вероятности и критичности возникновения рисков целостности, конфиденциальности и доступности. Описан метод итоговой оценки риска для клиента и рекомендации по его использованию.

Ключевые слова: *облачные вычисления, информационная безопасность, уязвимость, оценка риска.*

Barinov A.E., Ryabtseva O.V., Sokolov A.N.

ADAPTIVE CUSTOMER RISK ASSESSMENT IN CLOUD INFRASTRUCTURE

The paper is described the main security threats to cloud infrastructures according to NIST standard. The problem of risk assessment for a client using cloud infrastructure is considered. Previous approaches and standard models are described. The article proposes the joint use of the statistical approach and CVSS 3.0 vulnerability assessment in software products to calculate the disadvantages of compromising the cloud service. The approach involves a variety of assessments of the probability and severity of the occurrence of risks of integrity, confidentiality and availability. The method of final risk assessment for the client and recommendations for its use are described.

Keywords: *cloud computing, information security, vulnerability, risk assessment.*

Облачные вычисления - это модель обеспечения удобного повсеместного сетевого доступа по требованию к совместно используемому пулу конфигурируемых вычислительных ресурсов, которые можно быстро предоставить и внедрить с минимумом административных усилий или взаимодействия с сервис-провайдером.

Защита данных является важной проблемой, особенно для ресурсов облачного типа, предоставляемых дистанционно широкому кругу клиентов. Решение использования одних и тех же компьютеров, и программного обеспечения для разных целей разными пользователями является экономически обоснованным, но данный подход требует повышенного внимания к безопасности и разграничению прав, а также к балансировке нагрузки на аппаратную часть.

Модели обслуживания взаимосвязаны между собой вложенностью типов подписки IaaS-PaaS-SaaS. Таким образом, проблемы информационной безопасности для разных моделей сервиса в облаке имеют взаимосвязанный характер. То есть, при уязвимости на любом нижележащем, например уровне (IaaS), проблемы будут наследоваться и на более высокие слои.

Существуют несколько ведущих организаций, которые занимаются вопросами безопасности в облачных инфраструктурах:

– Альянс безопасности в «облаке» (Cloud Security Alliance, CSA);

– Европейское агентство сетевой и информационной безопасности (ENISA);

– Национальный институт стандартов и технологий (NIST).

Стандарт безопасности облачных вычислений (NIST Cloud Computing Security Reference Architecture), принятый в NIST, охватывает возможные потенциальные типы атак на сервисы облачных вычислений[1]:

– компрометация конфиденциальности и доступности данных, передаваемых облачными провайдерами;

– атаки, которые исходят из особенностей структуры и возможностей среды облачных вычислений для усиления и увеличения ущерба от атак;

– неавторизированный доступ потребителя (посредством некорректной аутентификации или авторизации, или уязвимостей, внесенных посредством периодического технического обслуживания) к ПО, данным и ресурсам, используемым авторизированным потребителем облачного сервиса;

– увеличение уровня сетевых атак, таких как DoS, эксплуатирующих ПО, при разработке которого не учитывалась модель угроз для распределенных ресурсов интернета, а также уязвимости в ресурсах, которые были доступны из частных сетей;

– ограниченные возможности по шифрованию данных в среде с большим количеством участников;

– переносимость, возникающая в результате использования нестандартных API, которые усложняют облачному потребителю возможность перехода к новому облачному провайдеру, когда требования доступности не выполняются;

– атаки, эксплуатирующие физическую абстракцию облачных ресурсов и недостатки в записях и процедурах аудита;

– атаки на виртуальные машины, которые не были соответствующим образом обновлены;

– атаки, эксплуатирующие нестыковки в глобальных и частных политиках безопасности.

Также стандарт выделяет основные задачи безопасности для облачных вычислений. Однако, наиболее специфическими для облачных инфраструктур являются следующие:

– защита от «цепных» (supply chain threats) угроз, включающая в себя подтверждение степени доверия и надежности сервис провайдера в той же степени, что и степень доверия используемого ПО и оборудования;

– задание доверенных границ между сервис-провайдером и потребителями для того, чтобы убедиться в ясности авторизованной ответственности за предоставление безопасности;

– поддержка переносимости, осуществляемой для того, чтобы потребитель имел возможность сменить облачного провайдера в тех случаях, когда у него возникает необходимость в части удовлетворения требований по целостности, доступности, конфиденциальности, включающая в себя возможность закрыть аккаунт в данный момент и копировать данные от одного сервис-провайдера к другому.

При этом стандарт NIST не описывает методик расчёта риска для облачных инфраструктур, а только перечисляет компоненты обеспечения безопасности в облачных инфраструктурах и уровни, на которых они должны быть реализованы, а также коэффициенты критичности для целостности, конфи-

денциальности и доступности для основных сценариев использования облачных технологий[1].

Стандарт ENISA[4] описывает 35 типовых сценариев развития рисков в облачных инфраструктурах, сопутствующие факторы их развития и подверженные рискам активы, оценивает вероятность и критичность каждого из них, предлагает модель оценки риска. Однако каждый из этих сценариев описан автономно. Стандарт не предполагает совместного развития сценариев и гибкой оценки риска для пользователей облачных ресурсов. Данное обстоятельство породило множество научных работ[2,3,5,6], посвящённых адаптивной оценке риска в облачных инфраструктурах. Но в современных источниках не дается исчерпывающее решение, которое обеспечивает адаптивную оценку риска для каждого клиента облачной инфраструктуры, а также обеспечивающую объективную оценку риска для клиента, защищённую от вмешательства сервис-провайдера. Известный подход[2] предполагает под собой оценку взаимного влияния программных компонентов на риск эксплуатации уязвимости и позволяет адаптивно рассчитать индекс безопасности для каждого клиента в зависимости от целей в обеспечении безопасности. Однако для его реализации требуется значительный ручной ввод экспертной информации, что повышает вероятность ошибочной оценки. Кроме того, в описываемом программном средстве отсутствует возможность интеграции с системой обнаружения уязвимостей. В другом известном подходе[3] описывается модель взаимного влияния уязвимостей в облачных инфраструктурах, однако она предполагает под собой небольшой набор из 15 правил взаимного влияния уязвимостей в программных компонентах для стандартного стека ПО. Данная модель не предполагает под собой детерминированную оценку риска для различных по критичности для разного типа угроз активов пользователей, использующих один и тот же стек ПО.

Подход[6] использует в качестве основы сценарии рисков ENISA[4], однако, для оценки вероятности возникновения угрозы использует методику на основе опросника CAIQ[7], что позволяет выполнить только экспертную оценку без учёта технических рисков, вызванных уязвимостями в программном обеспечении. Соответственно, даже при появлении технического описания уязвимости в открытых базах, невозможно оценить риск её влияния на конкретного пользователя облачной инфраструктуры.

Модель JRTM[5] (Joint Risk and Trust Model) предполагает оценку риска в зависимости от накопленной статистики сервис-провайдера по возникновению и устранению уязвимостей; оценку риска при наличии нескольких компонентов разной степени критичности и вероятности эксплуатации уязвимости, как у сервис-провайдера, так и у пользователя. Однако она не предполагает адаптацию оценки риска в зависимости от статуса уязвимости (наличие официального исправления, временного решения и т.д.), а также зрелости эксплойта и степени доступности информации об уязвимости. Также данная модель рассчитывает только вероятности возникновения угроз, вызванных уязвимостями, не учитывая степень их влияния на инфраструктуру, а также оценки степени риска уязвимостей из общедоступных баз CVE, DWF и других.

Рассмотрим выражение, для риска предложенное в модели JRTM:

$$\delta_f = r_f(1 - t_f) \tag{1}$$

Здесь указанная вероятностная оценка риска, состоящая из двух компонент r_f - вероятности возникновения угрозы, вызванной уязвимостью и t_f - вероятностью устранения уязвимости сервис-провайдером до тех пор, пока она не приведёт к инциденту информационной безопасности. Здесь и далее индекс $f \in \{\varepsilon; \phi; \rho\}$, что означает соответственно значения, относящиеся к целостности, конфиденциальности и доступности. При этом значение вероятности возникновения угрозы оценивается как:

$$r_{f(i)} = (1-\omega)R(f) + \omega\frac{f_i}{u_i} \tag{2}$$

где $R(f)$ случайная величина, основанная на функциях распределения вероятности, полученных из статистического анализа наблюдений за возникающими уязвимостями целостности, конфиденциальности и доступности. Модель JRTM является дискретной моделью и рассматривает время как набор периодов равной длины, где i – номер периода, а f_i - соответствующее ему количество клиентов сервис-провайдера, у которых возникла в этом периоде хотя бы одна уязвимость соответствующего типа, а u_i - суммарное количество клиентов, $\omega \in [0;1]$ - экспертная весовая оценка роли последнего периода.

Вероятность устранения уязвимости сервис-провайдером до тех пор, пока она не приведёт к инциденту информационной без-

опасности в работе[5] оценивается как:

$$t_f = \begin{cases} 0, & t_{sf} < 0 \\ 1, & t_{sf} > 1 \\ t_{sf}, & t_{sf} \in [0;1] \end{cases} \quad (3)$$

.

Оценка вероятности устранения уязвимости сервис-провайдером состоит из двух составляющих, основанных на долговременной статистике t_{fh} и кратковременной t_{fs} - за два последних периода, то есть:

$$t_{sf} = t_{fh} + t_{fs}, \quad (4)$$

Где долговременные оценки. вычисляются аналогично вероятности возникновения уязвимости:

$$t_{\varepsilon h(i)} = (1-\omega)R(\varepsilon_e) + \omega\frac{\varepsilon_{ei}}{\varepsilon_i}, \quad (5)$$

$$t_{\rho h(i)} = (1-\omega)R(\rho_e) + \omega\frac{\rho_{ei}}{\rho_i}, \quad (6)$$

$$t_{\phi h(i)} = \left((1-\omega)R(\phi_e) + \omega\frac{\phi_{ei}}{\phi_i}\right)^{R(D)} \quad (7)$$

.

Стоит отметить, что соответствующие значения f_{ei} - число клиентов, для которых уязвимости соответствующего типа, были предотвращены до того, как это повлекло возникновение инцидента в i периоде. $R(f_e)$ - соответствующие статистические распределения. В оценке конфиденциальности дополнительно включено распределение; $R(D)$, характеризующее количество периодов в течении которого существуют уязвимости конфиденциальности, то есть периодов течении которых возможна утечка информации.

Кратковременная оценка формируется как:

$$t_{fs(i)} = \begin{cases} d_{f(i)}^{\gamma}, & d_{f(i)} \geq 0 \\ -\sqrt[\gamma]{|d_{f(i)}|}, & d_{f(i)} < 0 \end{cases} \quad (8)$$

,

$$d_{f(i)} = \frac{f_{ei}}{f_i} - \frac{f_{e(i-1)}}{f_{i-1}} \quad (9)$$

.

где $\gamma \geq 1$ - экспертная тенденциозная оценка динамики деятельности провайдера по реакции на уязвимости.

При этом выражение (4) в работе[5] предполагает, что все уязвимости каждого класса устранимы за одинаковое время, однако уязвимости в программных продуктах могут иметь готовое решение для исправления, выпущенное производителем, либо временное решение, которое, возможно, должен реализовать провайдер, либо не иметь ничего из вышеперечисленного. Кроме того уязвимости могут иметь известный эксплойт, принцип его построения или не иметь такового. Зрелость эксплойта, уровень известности уязвимости, а также доступности её исправления влияют на скорость реакции сервис-провайдера по её исправлению, а также вероятность её эксплуатации. Используемый для оценки критичности уязвимостей в открытых базах стандарт CVSS 3.0[8] оценивает параметры: доступности исправления $t_{rl} \in [0.95;1]$ (нижнее значение – официальное исправление, верхнее его отсутствие или неизвестность его существования); зрелости эксплойта $t_{em} \in [0.91;1]$ (нижнее значение – наличие существования эксплойта не доказано, верхнее – имеется работоспособная версия); уровня доступности информации об уязвимости $t_{rc} \in [0.92;1]$ (нижнее значение – общедоступная информация об уязвимости не содержит технических деталей, верхнее – доступно детальное описание уязвимости). Ведение отдельной статистики по устранению различных категорий уязвимостей, значительно усложнит теоретический аппарат, кроме того в течение своего жизненного цикла уязвимость неоднократно меняет указанные выше параметры. Поэтому предлагается выполнять оценку t_{sf} как

$$t_{sf} = t_{fh} + t_{fs} + \sum_{j=1}^{n} 1 - t_{rlj} t_{emj} t_{rcj}. \quad (10)$$

В выражении (10) предполагается, что клиент или облачный провайдер подвержены одновременно n уязвимостям.

Если число сервисов используемых клиентом m, то его суммарная оценка вероятности возникновения инцидента[5]:

$$\varepsilon = 1 - \prod_{k=1}^{m}(1-\delta_{\varepsilon m}), \quad (11)$$

$$\phi = 1 - \prod_{k=1}^{m}(1-\delta_{\phi m}), \quad (12)$$

$$\rho = 1 - \prod_{k=1}^{m}\left(1 - \prod_{z=1}^{a_k}\delta_{\rho kz}\right). \quad (13)$$

Оценка доступности ρ отличается тем, что введён дополнительный параметр a_k - означающий общее количество сервисов или оборудования на которых может быть реализован тот же функционал клиента. Однако существует множество моделей[9,10] обеспечения и оценки доступности и данный вопрос заслуживает отдельной работы.

Фактор критичности уязвимостей для клиента может быть выражен, как:

$$I_{fs} = 1 - \prod_{k=1}^{n} (1 - I_{fk}) \quad , \qquad (14)$$

где I_{fk} - оценка критичности для целостности, конфиденциальности или доступности для соответствующей уязвимости в ПО. Данные значения содержаться в описании уязвимости по стандарту CVSS 3.0.

Тогда суммарный риск C_f можно выразить как совместную оценку его влияния и вероятности возникновения[6] или

$$C_{fs} = \frac{\lfloor 10 I_{fs} \rfloor + \lfloor 10 f \rfloor}{18} \quad . \qquad (15)$$

Суть (15) в том, что рейтинг маловероятных и малокритичных уязвимостей относительно снижается.

Для разных сервисов и разных клиентов возможны разные оценки критичности для разных составляющих информационной безопасности. Их клиент может оценить на основе своих бизнес-требований или опираясь на рекомендации, например[1]. Тогда в качестве итоговой оценки влияния уязвимостей можно получить следующее выражение:

$$C_s = 1 - (1 - C_\varepsilon R_\varepsilon)(1 - C_\phi R_\phi)(1 - C_\rho R_\rho) \, , \qquad (16)$$

где R_ε, R_ϕ, R_ρ - соответствующие оценки критичности целостности, конфиденциальности и доступности, связанные следующим соотношением:

$$R_\varepsilon + R_\phi + R_\rho = 1 \quad . \qquad (17)$$

Выражение (16) может быть применено клиентами облачных инфраструктур для оценки безопасности своих сервисов использующих облачные инфраструктуры сервис-провайдеров. Данные оценки могут быть получены, как для всего сервиса клиента, так и для каждого отдельно взятого используемого им сервис-провайдера, что может быть им использовано для выбора оптимального расположения ресурсов своих сервисов с точки зрения информационной безопасности при наличии нескольких сервис-провайдеров. Недостатками подхода является то, что во-первых статистические данные для выражений (2)-(9) может поставлять только сервис-провайдер с помощью системы мониторинга, следовательно здесь встаёт вопрос об обеспечении доверия к данным провайдера. Во – вторых, как отмечалось выше, возможно существование различных схем резервирования провайдеров, и для более точных оценок доступности этот факт следует учитывать.

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Примечания

[1] NIST Cloud Computing Security Reference Architecture, National Institute of Standards and Technology, Special Publication 500-299, May 2013.

[2] D. Dasgupta and M. Rahman, "A framework for estimating security coverage for cloud service insurance," in Proceedings of the 7th Annual Cyber Security and Information Intelligence ResearchWorkshop: Energy Infrastructure Cyber Protection (CSIIRW'11), Oak Ridge, Tenn, USA, October 2011

[3] I. Khalil, A. Khreishah, M. Azeem, Cloud computing security: a survey, Comput. (MDPI J.) 3 (1) (2014) 1–35, http://dx.doi.org/ 10.3390/computers3010001

[4] Cloud Computing: Benefits, risks and recommendations for information security, ENISA, November 2009

[5] Erdal Cayirci, Models for Cloud Risk Assessment: A Tutorial. Accountability and security in cloud, Springer April 2015, Vol. 8937 of series lecture notes in computer science, pp 154-184

[6] Cayirci, E., Garaga, A., Santana de Oliveira, A. et al. J Cloud Comp (2016) 5: 14. doi:10.1186/s13677-016-0064-x

[7] https://cloudsecurityalliance.org/group/consensus-assessments/

[8] Common Vulnerability Scoring System v3.0: Specification Document (v1.7)

[9] Availability Management Framework - Application Interface Specification SAI-AIS-AMF-B.04.01.

[10] Gonçalves G, Endo P, Rodrigues M, Sadok D, Curesco C Risk-based model for availability estimation of saf redundancy models. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7543848

Баринов Андрей Евгеньевич, аспирант кафедры инфокоммуникационные технологии, старший преподаватель кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, пр. Ленина, 76. E-mail: barinovae@susu.ru.

Barinov Andrey, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)", Chelyabinsk, Russian Federation. E-mail: barinovae@susu.ru.

Рябцева Ольга Викторовна, студентка ФГАОУ ВО «Южно-Уральский государственный университет» (национальный исследовательский университет). 454080, г. Челябинск, пр. Ленина, 76. E-mail: olyska33@mail.ru.

Ryabtseva Olga, student, "South Ural State University (national research university)", Chelyabinsk, Russian Federation. E-mail: olyska33@mail.ru.

Соколов Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», г. Челябинск. E-mail: SokolovAN@susu.ru.

Sokolov Alexander, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)", Chelyabinsk, Russian Federation. E-mail: SokolovAN@susu.ru.

УДК - 004.4.056 + 004.4.052 Вестник УрФО № 1(23) / 2017, с. 20–23

Югансон А.Н., Заколдаев Д.А.

РАЗРАБОТКА МЕТОДИКИ ДЛЯ РАСЧЕТА ОЦЕНКИ ТЕХНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ СРЕДСТВ

На сегодняшний день, программное обеспечение занимает ключевую роль во всех информационных процессах общества. Зачастую, вопросы надежности программного обеспечения задвигаются на второй план при проектировании и разработке программных средств в угоду скорейшего вывода программного продукта на рынок. В данной статье предлагается решение, позволяющие оценить технологическую безопасность разработанного продукта для дальнейшей минимизации рисков, связанных с его эксплуатацией и технической поддержкой.

Ключевые слова: *технологическая безопасность программных средств, надежность программного обеспечения, методика расчета оценки.*

Iuganson A., Zakoldaev D.

A CALCULATION METHODOLOGY OF ASSESS FOR SOFTWARE TECURITY

Nowadays software plays a key role in different information processes. However, software reliability becomes underestimated during its construction and developing. The deployment of new product may lead to various loss due to lack in software architecture and programming defects. In this article a new methodology was developed for calculation of assess for software tecurity. This metric may help to minimize economic risks on stages of exploitation and technical maintenance.

Keywords: *software reliability, software tecurity, calculation methodology.*

Вопросы технологической безопасности программных средств (ПС) с каждым днем становятся все более актуальными. По результатам аналитического исследования, проведенного компанией НПО «Эшелон» в 2012 году[1], были сделаны выводы: ситуация в области защищенности приложений не улучшается с течением времени. Менеджмент процесса разработки находится на низком уровне, что в свою очередь ведет к увеличению числа ошибок в программном коде и, как следствие, увеличению затрат на выпуск конечного продукта. По данным исследования, выполненного по заказу Национального института стандартов и технологий США, убытки, возникающие из-за слабого развития инфраструктуры устранения дефектов в ПО (уязвимостей и ошибок программирования), достигают 60 миллиардов долларов в год[2]. Стоимость устранения дефекта, пропущенного на этапах разработки и тестирования, может возрасти после поставки программы многократно[3].

Под технологической безопасностью ПС понимается совокупность свойств, характеризующих способность программы сохранять заданный уровень пригодности в заданных условиях в течение заданного интервала времени, где в качестве ограничения уровня пригодности рассматриваются дефекты безопасности и уязвимости[4].

Необходимо признать, что на сегодняшний день типовая методика для расчета оценки технологической безопасности ПС попросту отсутствует. Существующие работы (см. 5, 6) не могут обеспечить в должной мере повторяемость и воспроизводимость результатов испытания.

Таким образом, задача разработки и совершенствования методического обеспечения расчета оценки технологической безопасности ПС в настоящее время является актуальной.

Типовая методика расчета оценки (рис. 1) представляет собой вычисление определенного набора метрик, полученных при проведении испытаний. Для формирования множества типовых метрик была использована методика, предлагаемая стандартом ГОСТ 28195-89, оптимизированная с учетом особенностей исследуемых программных средств.

На первом этапе происходит вычисление расчетных элементов метрик:

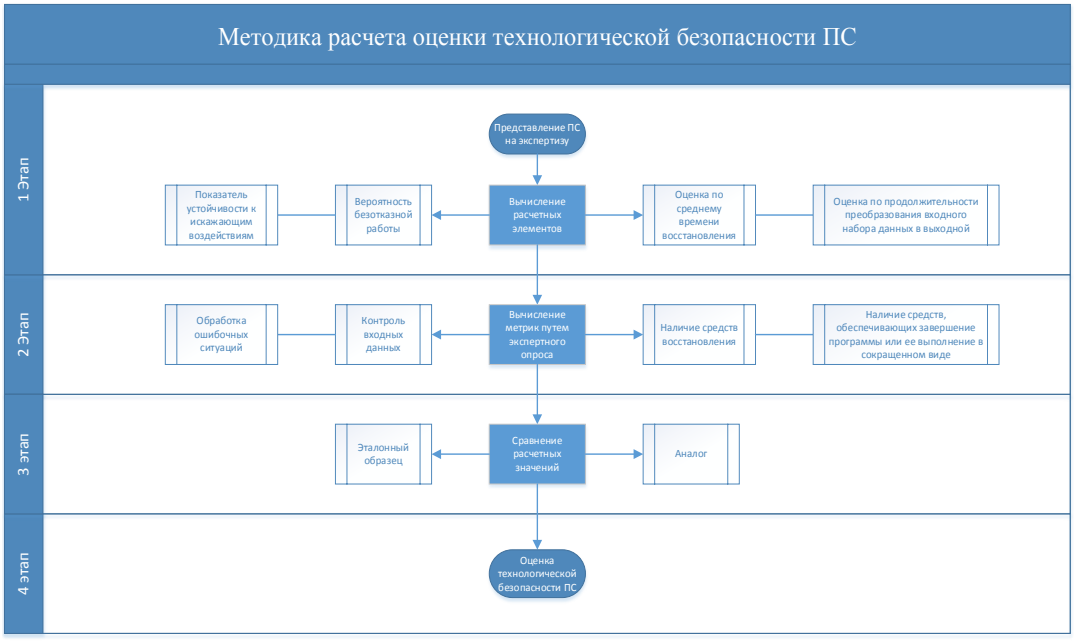


Рис. 1. Методика расчета оценки технологической безопасности ПС

– показатель устойчивости к искажающим воздействиям, вычисляемый по формуле:

$$P = 1 - \frac{D}{K} \qquad (1),$$

где D – число экспериментов, в которых искажающие воздействия приводили к отказу;

K – число экспериментов, в которых имитировались искажающие воздействия.

– вероятность безотказной работы, вычисляемая по формуле:

$$P = 1 - \frac{Q}{N} \quad (2),$$

где Q – число зарегистрированных отказов;

N – число экспериментов.

– оценка по среднему времени восстановления, вычисляемая по формуле:

$$Q_{\hat{a}} = \begin{cases} 1, \text{åñëè } \grave{O}_{\hat{a}} \le \grave{O}_{\hat{a}}^{\text{äîï}} \\ T_{\hat{a}}^{\text{äîï}} \big/ T_{\hat{a}}, \text{åñëè } \grave{O}_{\hat{a}} > \grave{O}_{\hat{a}}^{\text{äîï}} \end{cases} \quad (3),$$

где $\grave{O}_{\hat{a}}^{\text{äîï}}$ – допустимое среднее время восстановления;

$$\grave{O}_{\hat{a}} = \frac{1}{N}\sum_{i}^{N} T_{\hat{a}} \quad (4),$$

$\grave{O}_{\hat{a}}$ – среднее время восстановления, которое определяется по формуле:

где N – число восстановлений;

$T_{\hat{a}}$ –время восстановления после i-го отказа.

– оценка по продолжительности преобразования входного набора данных в выходной, вычисляемая по формуле:

$$Q_{\hat{a}} = \begin{cases} 1, \text{åñëè } \grave{O}_{\grave{n}} \le \grave{O}_{\grave{n}}^{\text{äîï}} \\ T_{\grave{n}}^{\text{äîï}} \big/ T_{\grave{n}}, \text{åñëè } \grave{O}_{\grave{n}} > \grave{O}_{\grave{n}}^{\text{äîï}} \end{cases} \quad (5),$$

где $\grave{O}_{\grave{n}}^{\text{äîï}}$ – допустимое время преобразования i-го входного набора данных;

$\grave{O}_{\grave{n}}$ – фактическая продолжительность преобразования i-го входного набора данных.

На втором этапе дается оценка метрикам, вычисляемым методом экспертного опроса (0 – ПС не удовлетворяет требованиям метрики, 1 – удовлетворяет):

– наличие требований к программе по устойчивости функционирования при наличии ошибок во входных данных;

– возможность обработки ошибочных ситуаций;

– полнота обработки ошибочных ситуаций;

– наличие тестов для проверки допустимых значений входных данных;

– наличие системы контроля полноты входных данных;

– наличие средств контроля корректности входных данных;

– наличие средств контроля непротиворечивости входных данных;

– наличие требований к программе по восстановлению процесса выполнения в случае сбоя операционной системы, процессора, внешних устройств;

– наличие требований к программе по восстановлению результатов при отказах процессора, ОС;

– наличие средств восстановления процесса в случае сбоя оборудования;

– наличие возможности разделения по времени выполнения отдельных функций программ;

– наличие возможности повторного старта с точки останова;

– наличие проверки параметров и адресов по диапазону их значений;

– наличий обработки граничных результатов;

– наличие обработки неопределенностей;

– наличие централизованного управления процессами, конкурирующими из-за ресурсов;

– наличие возможности автоматически обходить ошибочные ситуации в процессе вычисления;

– наличие средств, обеспечивающих завершение процесса решения в случае помех;

– наличие средств, обеспечивающих выполнение программы в сокращенном объеме в случае ошибок и помех.

На третьем этапе расчетные значения сравниваются с соответствующими базовыми значениями аналога или расчетного ПС, принимаемого за эталонный образец. В качестве аналогов выбираются реально существующие ПС того же функционального назначения, что и сравниваемое, с такими же основными параметрами, подобной структуры и применяемые в условиях эксплуатации.

На последнем этапе дается оценка технологической безопасности ПС. Общая оценка качества ПС в целом формируется экспертами по набору полученных значений оценок факторов надежности.

Таким образом, в ходе исследования была предложена методика для оценки технологи-

ческой безопасности ПС. Совокупность расчетных элементов метрик и метрик, вычисляемых методом экспертного опроса, позволяют оценить надежность ПС на стадии эксплуатации и технической поддержки. Это, безусловно, поможет снизить риски, связанные с отказом программного обеспечения на ранней стадии эксплуатации. Зачастую, данная оценка требуется значительно раньше, еще на стадии проектирования. Поэтому предложенная методика будет дорабатываться с целью охвата всех стадий разработки ПО.

Примечания

1. Сводный отчет по безопасности программного обеспечения в России и мире. М.:НПО «Эшелон», 2012. Вып.2. -URL: http://cnpo.ru/report_echelon_2012.pdf.

2. Gallaher M. P. and Kropp B. M. Economic impacts of inadequate infrastructure for software testing. Technical report, RTI International, National Institute of Standards and Technology, US Dept of Commerce, May 2002.

3. Forrest Shull, Vic Basili, Barry Boehm, Winsor A. Brown, Patricia Costa, Mikael Lindvall, Dan Port, Ioana Rus, Roseanne Tesoriero, and Marvin Zelkowitz. What we have learned about fighting defects. In International Software Metrics Symposium. Ottawa, Canada, 2002

4. Марков А.С. Немонотонные модели оценки надежности и безопасности функционирования программных средств на ранних этапах испытаний // Вопросы кибербезопасности. 2014. №2 (3).

5. Goel A. L., Okumoto K. Time-dependent error-detection rate model for software reliability and other performance measures //IEEE transactions on Reliability. – 1979. – Т. 28. – №. 3. – С. 206-211.

6. Patel D. Software Reliability: Models //International Journal of Computer Applications. – 2016. – Т. 152. – №. 9.

Югансон Андрей Николаевич, аспирант, ассистент кафедры проектирования и безопасности компьютерных систем, Университет ИТМО, 197101, г. Санкт-Петербург, Кронверкский проспект, д.49. E-mail: a_yougunson@corp.ifmo.ru

Заколдаев Данил Анатольевич, кандидат технических наук, доцент, заведующий кафедры проектирования и безопасности компьютерных систем, Университет ИТМО.
197101, г. Санкт-Петербург, Кронверкский проспект, д.49. E-mail: d.zakoldaev@mail.ru

Iuganson Andrei, PhD student, assistant of Department of Computer System Design and Security, ITMO University.
bld. 49, Kronverkskiy avenue, Saint-Petersburg, 197101, E-mail: a_yougunson@corp.ifmo.ru

Zakoldaev Danil, PhD in Technical Science, associate professor, head of Department of Computer System Design and Security, ITMO University.
bld. 49, Kronverkskiy avenue, Saint-Petersburg, 197101 E-mail: d.zakoldaev@mail.ru

УДК - 004.056 + 003.26 + 519.1:004.056 Вестник УрФО № 1(23) / 2017, с. 24–23

Геут К. Л., Титов С. С.

О РЕКУРРЕНТНЫХ СООТНОШЕНИЯХ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В работе рассматриваются соотношения, задающие нелинейные рекурсии первого порядка для общего линейного рекуррентного соотношения второго порядка с постоянными коэффициентами. Авторами получены условия существования некоторых нелинейных рекурсий первого порядка для линейных рекуррентных соотношений второго порядка с постоянными коэффициентами. Проведено отслеживание количества принимаемых переменными значений, что позволяет применить полученные результаты к линейным рекуррентным соотношениям между элементами не только числовых, но и конечных полей. Рассмотрены возможные криптографические приложения в информационной безопасности.

Ключевые слова: *рекуррентное соотношение, регистр сдвига, поточный шифр, марковская цепь.*

Geut K. L., Titov S. S.

ON RECURRENT RELATIONS IN INFORMATION SECURITY

The relations that define nonlinear recursions of the first order for a general linear second-order recurrence relation with constant coefficients are considered in the article. The authors have obtained the conditions for the existence of some nonlinear recursions of the first order and linear recurrence relations of the second order with constant coefficients. Tracking the number of decisions variables the values held, this allows us to apply the results to linear recurrence relations between the elements are not only numeric, but also the finite fields. The possible cryptographic applications in information security are obtained.

Keywords: recurrence relation, shift register, stream cipher, Markov chain.

Если рассматривать рекуррентные соотношения через их разностные уравнения, решением которых является последовательность элементов поля GF(q)[1], то в результате по начальным значениям можно построить бесконечную последовательность, причем каждый ее последующий член определяется из k предыдущих. Если представить значения элементов в виде 0 и 1 из поля GF(2), то последовательности такого вида легко реализуются на компьютере.

Одна из сфер применения линейных рекуррентных соотношений – это и генерация последовательностей псевдослучайных чисел. Обычно в реальных криптосхемах линейный регистр сдвига с обратной связью реализуется одной из двух различных конструкций, называемых, соответственно, регистрами Фибоначчи и Галуа, но все наиболее важные теоретические результаты применимы к обоим типам.

Еще один пример – рекуррентное распределение вероятностей марковских цепей[2], которые используются как математический аппарат для описания, например, процесса несанкционированной атаки, распознавания речи, аутентификации.

Использование рекуррентных соотношений над конечными полями для М-последовательностей при генерации гаммы шифров дает максимальный период, что влияет на стойкость шифра. Криптостойкость поточных шифров полностью зависит от качества генератора потока ключей. Большинство современных генераторов гаммы построено на линейных регистрах сдвига (ЛРС). Главная проблема при проектировании структуры ЛРС – это достижение максимального периода повтора ЛРС, потому что повтор состояния ЛРС означает, что и гамма будет периодически повторяться, что снижает криптостойкость системы. Для ЛРС длиной n бит максимальный период составляет $2^n - 1$ тактов (состояние, когда все биты равны нулю, недопустимо, поскольку ЛРС любой структуры не выходит из этого состояния, зацикливаясь в нем).

Существуют генераторы, порождающие нелинейные рекуррентные последовательности, такие генераторы по своим диагностическим свойствам отличаются от линейных. В частности, в n-разрядном нелинейном генераторе достаточно просто порождается двоичная последовательность де Брейна. Она представляет собой нелинейную двоичную последовательность x_i периода $T = 2^n$, в которой всевозможные векторы $(x_j, x_{j+1}, \ldots x_{j+n-1})$ длины n при любом j встречается только один раз. Исключение запрещенного нулевого состояния всех триггеров генератора позволяет увеличить период формируемой последовательности и сделать его максимально возможным, равным 2^m, повысить ее качество, так как вероятности появления 0 и 1 становятся равными 0,5. На основе таких последовательностей построен, в частности, циклический избыточный код CRC32.

Одна из классических задач рекуррентных последовательностей – числа Фибоначчи, которые удовлетворяют линейному рекуррентному соотношению второго порядка. В работе В. Н. Ушакова[3] была поставлена и решена задача построения нелинейной рекурсии первого порядка для таких чисел: $u_{n+2} = u_{n+1} + u_n$.

$$u_{n+1} = \frac{1}{2}u_n + \frac{1}{2}\sqrt{5u_n^2 - 4}\ , \text{ при нечетном n,} \quad (1)$$

$$u_{n+1} = \frac{1}{2}u_n + \frac{1}{2}\sqrt{5u_n^2 + 4}\ , \text{ при четном n.} \quad (2)$$

Общая задача понижения порядка рекуррентного соотношения ставится для произвольной рекурсии.

Рассмотрим линейное уравнение конечных разностей 2-го порядка с постоянными коэффициентами и без правой части[1].

$$f_{x+2} + a_1 f_{x+1} + a_2 f_x = 0. \quad (3)$$

Один из примеров решения такого уравнения – числа Фибоначчи:

$$u_{n+2} = u_{n+1} + u_n, \quad (4)$$

где $u_1 = u_2 = 1$[1].

Решаем это рекуррентное соотношение стандартным образом[1] и получаем итоговую формулу:

$$x = u_n = \ddot{e}^n = \frac{f_n \pm \sqrt{f_n^2 - 4a_2^n C_1 C_2}}{2C_1}. \quad (5)$$

Если $a_2 = 1$, то x есть функция одной переменной f_n при постоянных C_1 и C_2.

Если $a_2 = -1$, то x есть функция одной переменной f_n, но разного вида для четных и нечетных n.

Если $a_2^3 = 1$, т.е. порядок a_2 равен трем, то x есть функция одной переменной f_n, но трех видов, в зависимости от остатка деления n на три.

Если $a_2^4 = 1$ (например, $a_2 = i$), т.е. порядок a_2 равен четырем, то x есть функция одной переменной f_n, но четырех видов и т.д.

Если же порядок a_2 бесконечный, то нет единой формулы, и x есть функция двух переменных f_n и n.

Предположим, что порядок a_2 конечный. Решение задачи построения рекурсии первого порядка аналогично задаче нахождения промежуточных интегралов первого порядка для дифференциальных уравнений второго порядка. В этом случае получаем

$$f_{n+1} = C_1 \ddot{e}^{n+1} + C_2 \frac{a_2^{n+1}}{\ddot{e}^{n+1}} \quad (6)$$

Это и есть решение в общем виде.

$$f_{n+1} = C_1 \frac{f_n + \sqrt{f_n^2 - 4a_2^n C_1 C_2}}{2C_1} \ddot{e} + C_2 \frac{2C_1 a_2^{n+1}}{\ddot{e}(f_n + \sqrt{f_n^2 - 4a_2^n C_1 C_2})} \quad (7)$$

Утверждение 1. Если в квадратном уравнении $\lambda^2 + a_1\lambda^1 + a_2 = 0$ порядок свободного члена конечен и равен *p*, то для решения рекуррентного соотношения при заданных C_1, C_2 корень $x = \lambda^n$ является функ- $f_{n+1} = C_1 \ddot{e}_1^{n+1} + C_2 \ddot{e}_2^{n+1}$ цией одной переменной fn и задается формулой p видов.

Более общая задача, когда $\lambda = 0$ или $\lambda = 1$ тоже сводится к зависимости первого порядка. В общем случае требуется описать, какие должны быть коэффициенты характеристического уравнения, чтобы существовала зависимость в виде многочлена.

Так, квадратичная зависимость, вида

$$F(f_n, f_{n+1}) = af_n^2 + bf_nf_{n+1} + cf_{n+1}^2 + df_n + ef_{n+1} = C = Const \quad (8)$$

имеет место при

$$fn = C1\lambda_1^n + C2\lambda_2^n,$$
$$= u \qquad = v$$
$$fn+1 = C1\lambda_1^{n+1} + C2\lambda_2^{n+1}.$$
$$= \lambda 1u \qquad = \lambda 2v$$

Эта зависимость (8) при $\lambda_1 = -1, \lambda_2 \notin \{0,1,-1\}$ существует в виде $\lambda_2^2 f_n^2 - 2\lambda_2 f_n f_{n+1} + f_{n+1}^2 = C$ (9)

для рекуррентного соотношения

$$f_{n+2} - (\lambda_2 - 1)f_{n+1} - \lambda_2 f_n = 0 \quad (10)$$

Кубическая зависимость первого порядка вида

$$F(f_n, f_{n+1}) = af_n^2 + bf_nf_{n+1} + cf_{n+1}^2 + df_n + ef_{n+1} = C = Const \quad (11)$$

должна выполняться тождественно по n для функций

$$fn = C_1\lambda_1^n + C_2\lambda_2^n = u + v,$$
$$fn+1 = C_1\lambda_1^{n+1} + C_2\lambda_2^{n+1} = \lambda_1 u + \lambda_2 v,$$
$$(\lambda_1 \neq \lambda_2)(\lambda_i \notin \{0,1,-1\}) \quad (\lambda_1\lambda_2 \neq 1)$$

Решение на основании определителей типа Вандермонда показывает, что такая зависимость может иметь место, только если либо $\lambda_1 = \lambda_2$, либо $\lambda_1 = 1$, либо $\lambda_2 = 1$, чего не может быть по предположению.

Итак, доказано

Утверждение 2. Кубическая зависимость (11) имеет место (при отсутствии квадратичной), только в случае, когда корни λ_1, λ_2 характеристического уравнения удовлетворяют либо уравнению $\lambda_1^2\lambda_2 = 1$, либо уравнению $\lambda_1\lambda_2^2 = 1$. При этом зависимость оказывается однородной.

Использование рекуррентных соотношений дает эффективный метод решения многих комбинаторных задач. В криптографии рекуррентные соотношения используются для генераторов псевдослучайных последовательностей.

Проведённое выше отслеживание количества принимаемых переменными значений позволяет применить полученные результаты и к линейным рекуррентным соотношениям между элементами не только числовых, но и конечных полей. Так, обобщение соотношения Чебышёва для многочленов Чебышёва-Диксона[5,6] может прояснить проблему с простыми числами Ферма[7] для которых задача дискретного логарифмирования предполагается быстро решаемой.

Примечания

1. Гельфонд А. О. Исчисление конечных разностей / М.: Наука, 1967. – 376 с.

2. Марков А. А. Исчисление конечных разностей / Одесса : Типография Акционерного Южно-Русского Общества Печатного Дела, 1910.

3. Ушаков В. Н. Египетские треугольники и числа Фибоначчи // Империя математики. – №1. – 2001. – С. 21–60.

4. Геут Кр. Л., Титов С. С. Задача, эквивалентная проверке простоты чисел Ферма // Прикладная дискретная математика (Приложение). – Томск: ТПУ. 2014. – № 7. – С. 13–14.

5. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. – М. : КомКнига, 2012. – 328 с.

6. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. – М. : КомКнига. 2006. – 280 с.

7. Геут К. Л., Титов С. С. О задаче построения нелинейных рекуррентных соотношений // IV междисциплинарная молодежная научная конференция УрО РАН «Информационная школа молодого ученого» : сб. научных трудов ЦНБ УрО РАН. – Екатеринбург, 2014. – С. 203–208.

8. Бабаш А. В., Шанкин Г. П. Криптография. под редакцией В. П. Шерстюка, ЭЛ. Применко – М. : СОЛОН-ПРЕСС. 2007 – 512 С.

ГЕУТ Кристина Леонидовна, ассистент Уральского государственного университета путей сообщения, 620034, Екатеринбург, ул. Колмогорова, д. 66, E-mail: geutkrl@yandex.ru

ТИТОВ Сергей Сергеевич, профессор Уральского государственного университета путей сообщения, докт. физ-мат. наук, профессор, 620034, Екатеринбург, ул. Колмогорова, д. 66, E-mail: sergey.titov@usaaa.ru

GEUT Kristina Leonidovna, Assistant professor of the Ural State University of Railway Transport, 620034, 66 Bld., Kolmogorova Str., Ekaterinburg, E-mail: geutkrl@yandex.ru

TITOV Sergey Sergeevich, Professor of the Ural State University of Railway Transport, Doctor of Physical and Mathematical Sciences, Professor, 620034, 66 Bld., Kolmogorova Str., Ekaterinburg, E-mail: sergey.titov@usaaa.ru

УДК - 004.056 + 005. 334:004.056 Вестник УрФО № 1(23) / 2017, с. 24–31

Зырянова Т. Ю.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ОЦЕНКИ И ПРОГНОЗИРОВАНИЯ РИСКОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Понятия оценки рисков и управления рисками появились относительно недавно и сегодня вызывают постоянный интерес специалистов как в области обеспечения непрерывности бизнеса, так и в области информационной безопасности.

Использование информационных технологий всегда связано с определенной совокупностью рисков, под которыми обычно понимается количественная оценка событий, ведущих к финансовым потерям.

В наиболее распространенном понимании этой проблемы процесс управления информационными рисками представляет собой действия по идентификации угрозы, оценке вероятности появления угрозы, количественной оценке ущерба в случае осуществления угрозы, выработке контрмер и оценке их эффективности.

В статье приводится постановка задачи анализа информационных рисков; анализ международной концепции информационной безопасности и особенностей ее применения; анализ теоретических и практических подходов к оценке и прогнозированию информационных рисков.

Ключевые слова: *система менеджмента информационной безопасности, риск информационной безопасности, анализ риска, оценка риска, прогнозирование риска, количественная оценка риска.*

Zyryanova T. Yu.

COMPARATIVE ANALYSIS OF METHODS FOR RISK ASSESSMENT AND RISK FORECASTING FOR INFORMATION SYSTEMS

The concept of risk evaluation and risk management have emerged relatively recently and today cause a constant interest of specialists both in the business continuity and in the information security.

The use of information technology is always associated with a certain set of risks, which are usually understood as the estimation of events leading to financial losses.

In the most common understanding of this problem, the process of information risk management is the actions for identifying a threat, evaluation the probability of a threat, quantifying the damage in the event of a threat, developing countermeasures and assessing their effectiveness.

The article presents the task of analyzing information risks; the analysis of the international concept of information security and features of its application; the analysis of theoretical and practical approaches to the assessment and forecasting of information risk.

Keywords: *information security management system, information security risk, risk assessment, risk forecasting, risk evaluation.*

Современный уровень развития информационных технологий выдвигает на передний план новые требования к построению систем защиты информации и обеспечению информационной безопасности.

На протяжении длительного времени понятие информационной безопасности отождествлялось с обеспечением конфиденциальности информации, а наибольшее распространение получило применение технических средств защиты. Сегодня информация, будучи нематериальной по своей природе, становится предметом товарно-денежных отношений и объектом нормативно-правового регулирования. Перед государственными и коммерческими предприятиями и организациями все острее встает проблема не только обеспечения надежной защиты информации от несанкционированного ознакомления и распространения, но и поддержки стабильного доступа к информации и возможности эффективной работы с ней.

Актуальность исследований в данной области обусловлена высокими темпами развития и расширения сферы применения информационных технологий, которые значительно опережают формирование теоретической и методологической базы построения систем управления информационной безопасностью.

Потери от нарушения информационной безопасности зачастую превышают затраты на создание и эксплуатацию систем защиты.

Создаваемые системы менеджмента информационной безопасностью должны быть основаны на анализе рисков информационных систем (а именно на оценке текущего уровня риска и прогнозировании этого уровня в будущем).

Эффективные методики оценки и прогнозирования информационных рисков на сегодняшний день отсутствуют, но именно они должны помочь ответить на вопросы:

– какая информация подлежит защите и по каким причинам;

– к чему может привести отсутствие эффективной системы защиты информации;

– как организовать наиболее эффективную систему защиты информации;

– какова ее стоимость.

Под системой менеджмента информационной безопасности (СМИБ) понимается часть общей системы менеджмента, базирующаяся на анализе рисков и предназначенная для проектирования, реализации, контроля, сопровождения и совершенствования мер в области информационной безопасности.

Под термином «риск» будем понимать отрицательное следствие наличия уязвимости, характеризующееся вероятностью возникновения негативного события и последствиями возникновения этого события.

В основу исследования положено предположение о том, что СМИБ должна базироваться на анализе рисков с целью наибольшей ее эффективности.

Для достижения этой цели необходимо решить следующие задачи.

Первая задача связана с тем, что формирование модели угроз должно носить динамический характер. Какое бы множество угроз не было сформировано, всегда есть возможность появления новой, неизвестной ранее угрозы в неопределенный заранее момент времени. Предпосылки таких событий в модели угроз необходимо учитывать.

Вторая задача состоит в разработке методики оценки и прогнозирования информационного риска, что в сумме и составляет процесс анализа информационного риска.

При решении третьей задачи необходимо оценить эффективность построенной методики на конкретных моделях или примерах информационных систем.

1. Базовая терминология и основные положения теории управления информационными рисками

Базовая терминология теории управления информационными рисками на сегодняшний день сформирована в системе международных стандартов ISO/IEC 27000, которые гармонизированы в Российской Федерации в серии ГОСТ Р ИСО/МЭК 27000, например [1 – 4].

Понятие информационного риска наглядно иллюстрирует схема, приведенная на рис. 1.

Рис. 1. Составляющие информационного риска

Угрозой называется потенциальная причина нежелательного инцидента, который может причинить ущерб информационному ресурсу.

Уязвимость – слабость в системе защиты, дающая возможность реализации угрозы.

Стрелки на рис. 1 указывают направление роста следующих показателей:

– для ресурса – его ценность;

– для угрозы – вероятность ее реализации;

– для уязвимости – простота, с которой уязвимость используется.

Существует ряд общепринятых подходов к измерению рисков. Наиболее распространенные из них – оценка по двум факторам и оценка по трем факторам. Формула (1) иллюстрирует подход вычислению риска по трем факторам (здесь не указаны единицы измерения ущерба, так как зачастую невозможно оценить ущерб в его материальном выражении. Он может быть обусловлен, например, потерей репутации компании, причинением вреда жизни и здоровью людей, террористической угрозой).

$$R = P \cdot P_y \cdot V, \qquad (1)$$

где R – риск, P – вероятность реализации угрозы, P_y – вероятность того, что уязвимость будет использована; V – размер возможного ущерба или ценность ресурса.

Если переменные в (1) являются количественными величинами (выраженные, например, в денежных единицах), то риск – это математическое ожидания размера ущерба.

Если переменные являются качественными величинами (оценка производится относительно *низкого, среднего, высокого* уровней некоторой шкалы измерения), то метрическая операция умножения не определена. Таким образом, в явном виде эта формула использоваться не может, а рассматривается лишь как формулировка общей идеи. В этом случае применяются разного рода табличные методы оценки риска.

Пример табличного метода приведен на рис. 2. Здесь вероятность возникновения угрозы и вероятность использования уязви-

Вероятность возникновения угрозы		**Низкая**			**Средняя**			**Высокая**		
Вероятность использования уязвимости		**Н**	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Низкий риск: *0 – 2*
Средний риск: *3 – 5*
Высокий риск: *6 – 8*

Рис. 2. Табличный метод оценки ценности ресурса, характеристик угроз и уязвимостей

мости оцениваются по трехуровневой шкале, ущерб – по пятиуровневой и итоговый риск – по 9-уровневой [4].

После того как оценки риска получены для каждой известной угрозы, они должны быть интегрированы в итоговый показатель.

В соответствии с приведенным подходом информация, подлежащая защите на конкретном предприятии или в организации классифицируется на основе утвержденной системы классификации, например:

– информация, составляющая коммерческую тайну предприятия (организации);

– персональные данные;

– информация, составляющая служебную тайну и т. д.

Для каждого класса защищаемой информации формируется модель угроз, определяется их актуальность, размер возможного ущерба.

Например, к угрозам несанкционированного доступа могут быть отнесены:

– угрозы, реализуемые с применением программных средств операционной системы;

– угрозы, реализуемые с применением специального программного обеспечения;

– угрозы, реализуемые с применением вредоносных программ.

Аналогично определяются и оцениваются уязвимости по различным направлениям безопасности (табл. 1).

Для выявления угроз и уязвимостей используются следующие методы:

– автоматизированные инструментальные средства поиска уязвимостей;

– тестирование на проникновение;

– проверка кодов;

– опрос сотрудников и пользователей;

– физический осмотр;

– анализ документов.

После всех проведенных классификаций и оценок полученные результаты сводятся в таблицу, аналогичную приведенной на рис. 2, по которой определяется итоговый уровень риска.

Очевидно, что такие методики не всегда могут быть эффективны.

Таблица 1

Примеры уязвимостей информационных систем

Класс уязвимостей	Примеры уязвимостей
Аппаратные средства	Недостаточное техническое обслуживание Отсутствие эффективного контроля изменений конфигурации Незащищенное хранение
Программные средства	Отсутствующее или недостаточное тестирование программных средств Неверное распределение прав доступа Незащищенные таблицы паролей
Сеть	Незащищенные линии связи Ненадежная сетевая архитектура Передача паролей в незашифрованном виде
Персонал	Неадекватные процедуры набора персонала Недостаточное осознание требований безопасности Безнадзорная работа внешнего персонала

2. Постановка задачи оценки и прогнозирования информационного риска

Исходя из вышеизложенных фактов, будем рассматривать задачу оценки и прогнозирования информационного риска в следующих предположениях.

1. Невозможно сформировать полные множества угроз и уязвимостей.

2. Множества угроз и уязвимостей формируются динамически.

3. Элементы множества угроз и множества уязвимостей могут быть взаимосвязаны.

4. Суммарный риск в информационной системе зависит от множества параметров (2).

$$R = F(f_1, f_2, \ldots, f_N). \qquad (2)$$

Параметров, формирующих риск, может быть сколь угодно много, и выявить функциональную зависимость не представляется возможным.

Итак, для решения задачи оценки и прогнозирования информационного риска требуется:

– получить оценку текущего значения риска;

– построить прогноз значения риска на

будущий интервал времени в случае сохранения уровня защищенности информации;

– построить прогноз значения риска на будущий интервал времени при изменении уровня защищенности информации.

3. Метод решения задачи оценки и прогнозирования информационного риска на основе нечеткой логики

Первый метод решения поставленной задачи основан на применении нечетко-логического подхода.

Основное положение этого метода состоит в получении количественной оценки уровня риска, возникающего в результате неполного выполнения *функции безопасности* – функциональной возможности части системы информационных технологий или продукта информационных технологий, обеспечивающих выполнение требований информационной безопасности.

Алгоритм получения оценки строится на основании следующих предположений:

– имеется набор оценок уровней выполнения функций безопасности Y_i;

– необходимо получить количественную оценку R – текущего уровня риска;

– имеется набор лингвистических термов, характеризующих значения входных и выходного параметров;

– так как число элементов множества Y велико, а их вклад в изменение значений выходного параметра невозможно выразить функционально, задача получения оценки уровня риска решается путем построения системы нечеткого логического вывода (НЛВ).

На *первом этапе* решения задачи определяются входные и выходной параметры системы НЛВ:

y_i, $i=1, 2, \ldots, M$ – входные параметры (текущие уровни выполнения функций безопасности);

r – выходной параметр (текущий уровень риска);

Ni – количество термов для yi ;

N – количество термов для r;

На *третьем этапе* решается задача построения функций принадлежности, результат которой приведен на рис. 3.

	низкий	средний	высокий
[0..0,1)	1	0	0
[0,1..0,2)	0,8	0,4	0
[0,2..0,3)	0,6	0,8	0
[0,3..0,4)	0	1	0,2
[0,4..0,5)	0	0,6	0,4
[0,5..0,6)	0	0,4	0,8
[0,6..0,7)	0	0	1
[0,7..0,8)	0	0	1
[0,8..0,9)	0	0	1
[0,9..1]	0	0	1

Рис. 3. Функции принадлежности нечетких множеств

На *четвертом этапе* определяются значения функций принадлежности, соответствующие оценкам текущих значений входных параметров. На рис. 4 приведен пример для двух входных параметров.

На пятом этапе определяются степени истинности $\tilde{R}_{\delta_{k_1,k_2,\ldots,k_M}}$, $(k_i \in [1, N_i], i \in [1, M])$ для каждого из продукционных правил (рис. 5).

На *шестом этапе* строится результирующая функция принадлежности $\hat{R}(r)$ для выходного параметра с учетом степеней истинности всех продукционных правил. Она опре-

$$\{\alpha_1^i, \alpha_2^i, \ldots, \alpha_{N_i}^i\} = \{"íèçêèé\ ", \ldots, "âûñîêèé\ "\}$$ – терм-множества для yi ;

$$\{\delta_1, \ldots, \delta_N\} = \{"íèçêèé\ ", \ldots, "âûñîêèé\ "\}$$ – терм-множество для r .

На *втором этапе* строится нечеткая база знаний в виде набора продукционных правил

($F: \prod \{\alpha_k^i : k \in [1, N_i]\} \to \{\delta_j : j \in [1, N]\}$, где M – количество элементов множества Y, N – количество термов параметра R, N_i – количество термов параметра Y_i), для которых предполагаются заданными функции принадлежности нечетких множеств.

деляется как максимум значений степеней истинности всех продукционных правил для текущего значения r (рис. 6).

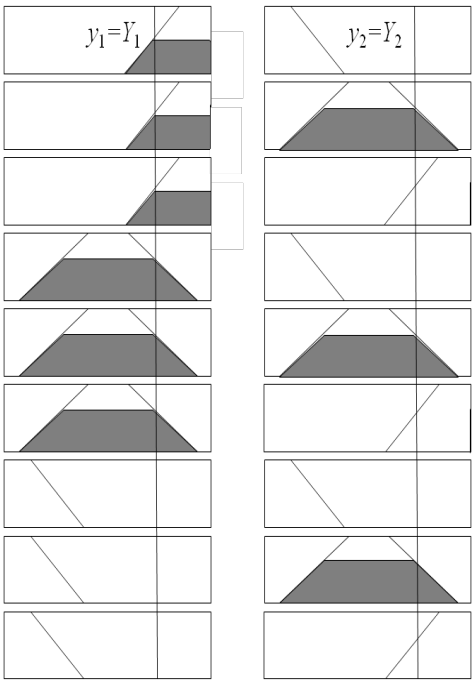


Рис.4. Определение значений функций принадлежности, соответствующих оценкам y_i

$$\widetilde{R}_{\delta_{k_1,k_2,\ldots,k_M}} = \bigcap_{i=1}^{M} \widetilde{P}_{\alpha_{k_i}^i} = \min\{\widetilde{P}_{\alpha_{k_i}^i}\}$$

$$k_i \in [1, N_i], \quad i \in [1, M]$$

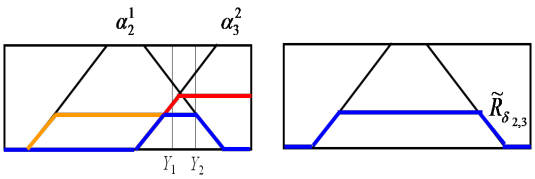
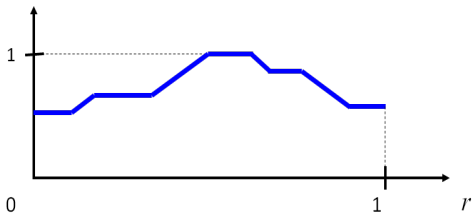


Рис. 5. Степени истинности продукционных правил



$$\overline{R}(r) = \bigcup_{k_i \in [1,N_i]} \widetilde{R}_{\delta_{k_1,k_2,\ldots,k_M}} = \max\{\widetilde{R}_{\delta_{k_1,k_2,\ldots,k_M}}(r) : r \in [0,1]\}$$

Рис. 6. Объединение результатов (функция принадлежности для r)

На заключительном *седьмом этапе* вычисляется результирующее значение R функции принадлежности выходного параметра путем дефаззификации (3).

$$R = \frac{\int_r r \cdot \overline{R}(r) d}{\int \overline{R}(r) d}. \quad (3)$$

Этот метод частично решает проблему множественности факторов формирования риска, но содержит большой объем экспертных данных, которые не всегда объективны.

4. Статистический метод решения задачи оценки и прогнозирования информационного риска

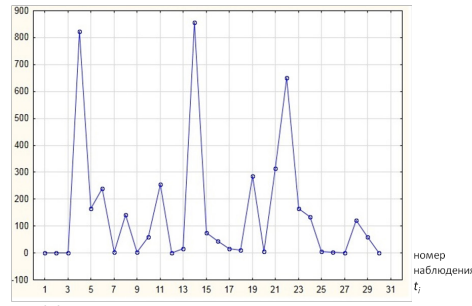
Второй метод решения поставленной задачи строится на основании следующих предположений:

1) уровень информационного риска определяется совокупностью факторов различного характера;

2) изменение уровня риска является случайным событием.

Динамический процесс формирования риска будем рассматривать как случайный процесс и моделировать его при помощи временного ряда.

На рис. 7 показан временной ряд, полученный на основании измерений времени бездействия компонента системы защиты информации.

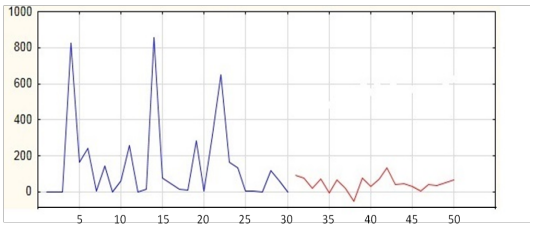


$x_i = x(t_i) = f(t_i) + \varepsilon_i$; $f(t)$ - систематическая составляющая ε - случайная составляющая

Рис. 7. Последовательность измерений значений переменной (процесса) за определенный период времени через одинаковые промежутки

Методы анализа временных рядов позволяют выявить в таком процессе долгосрочную тенденцию – тренд и так называемую сезонную компоненту на основе анализа автокорреляций.

На основе модели ARIMA (авторегрессии и проинтегрированного скользящего среднего) получаем прогноз значений временного ряда на будущие периоды времени (рис. 8).



$$x_i = a_1 x_{i-1} + a_2 x_{i-2} + \ldots + a_p x_{i-p} + b_1 \varepsilon_{i-1} + b_2 \varepsilon_{i-2} + \ldots + b_q \varepsilon_{i-q} + \varepsilon_i,$$

где $a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q$ - коэффициенты модели ARIMA

Рис. 8. Прогноз поведения временного ряда

Мы видим типичный результат применения метода прогнозирования временных рядов к процессу формирования информационного риска. Правильный подбор параметров модели оценивания даст корректный результат в случае большого объема выборки. Выявить закономерности в таких процессах достаточно сложно. В связи с этим предлагается еще один метод, который дает более точные результаты.

5. Метод решения задачи оценки и прогнозирования информационного риска на основе вейвлет-анализа

Этот метод основан на следующих особенностях процесса формирования риска.

1. Периодичность. Однако следует учитывать, что комбинация колебаний может быть настолько сложной, что выявить их наличие традиционными статистическими методами не представляется возможным.

2. Наличие тренда, который также может быть неочевидным.

3. Наличие локальных особенностей (резкие, скачкообразные изменения характеристик), носящих как случайный, так и систематический характер.

Вейвлет-анализ обычно применяется для исследования сложных данных и позволяет выявить различные свойства сложного процесса.

Производится разложение временного ряда по базису, образованному сдвигами и масштабированием функции-прототипа (вейвлета), для которого характерны колебания около оси абсцисс и быстрое убывание к нулю по мере роста модуля аргумента (рис. 9).

Вычисляется скалярное произведение исследуемых данных с различными сдвигами вейвлета на разных масштабах. В результате получается набор коэффициентов, показывающих, насколько поведение процесса в данной точке похоже на поведение вейвлета (чем больше коэффициент, тем больше близость.

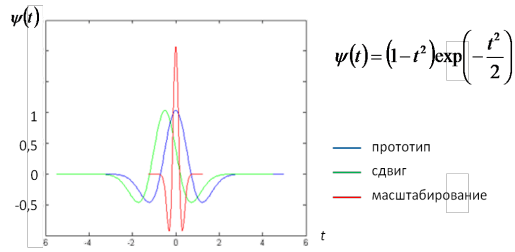


Рис. 9. Сдвиг и масштабирование вейвлета

Коэффициенты наносятся на карту, где по оси абсцисс отложены сдвиги вейвлета, а по оси ординат – масштабы, в виде точек различной яркости.

Всплески яркости показывают наличие периодических колебаний. Смещение всплесков вдоль оси масштабов говорит об изменении частоты колебаний (рис. 10).

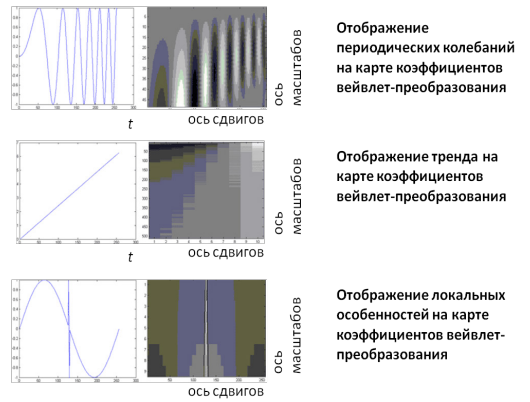


Рис. 10. Отображение особенностей исследуемого процесса на карте вейвлет-преобразования

Тренд на карте отображается как плавное изменение яркости вдоль оси сдвигов одновременно на всех масштабах. Также можно отследить наличие нескольких последовательных трендов.

Локальные особенности на карте представлены как линии резкого перепада яркости.

Таким образом, каждый фактор процесса формирования риска даст характерный отпечаток на карте вейвлет-преобразования.

6. Полученные результаты и выводы

В результате проведенного исследования:

– сформулирована задача анализа информационных рисков;

– проведен анализ международной кон-

цепции информационной безопасности и особенностей ее применения;

– проведен анализ теоретических и практических подходов к оценке и прогнозированию информационных рисков;

– приведена оценка применимости методов вейвлет-анализа к решению поставленной задачи.

Основная проблема решения задач анализа информационных рисков заключается в неполных и неточных исходных данных о характере воздействия угроз информационной безопасности.

Существующие методы анализа информационных рисков не позволяют получать количественные оценки уровня риска с приемлемой точностью.

Существует необходимость разработки количественных методик оценки и прогнозирования информационных рисков в условиях неопределенности воздействия угроз информационной безопасности.

Примечания

1. ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология. Средства обеспечения безопасности. Системы управления информационной безопасностью. Общий обзор и терминология».

2. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Средства обеспечения безопасности. Системы управления информационной безопасностью. Требования».

3. ГОСТ Р ИСО/МЭК 27004-2011 «Информационная технология. Средства обеспечения безопасности. Управление информационной безопасностью. Измерения».

4. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Средства обеспечения безопасности. Управление рисками информационной безопасности».

ЗЫРЯНОВА Татьяна Юрьевна, заведующий кафедрой «Информационные технологии и защита информации» Уральского государственного университета путей сообщения», канд. тех. наук. 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: tzyryanova@usurt.ru

ZYRYANOVA Tatiana, Chief of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorova str., Yekaterinburg, 620034. E-mail: tzyryanova@usurt.ru

УДК - 341.01:004.056 + 341.1:004.056 Вестник УрФО № 1(23) / 2017, с. 32–39

Ефремов А.А.

РАЗВИТИЕ ПРАВОВОГО ИНСТИТУТА МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья посвящена анализу современных тенденций развития международной информационной безопасности как института международного права. Рассмотрены доклады Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2013 и 2015 г.г., международные соглашения в сфере международной информационной безопасности, а также Рекомендация ОЭСР по управлению рисками цифровой безопасности для экономического и социального процветания 2015 г.

Ключевые слова: *информационная безопасность; международное право; международные организации; Организация Объединенных Наций; Организация экономического сотрудничества и развития*

Yefremov A.A.

EVOLUTION OF LEGAL INSTITUTE OF INTERNATIONAL INFORMATION SECURITY

The article is devoted to analysis of modern trends of the development of international information security law as an institute of international law. The reports of the Groups of Governmental Experts of the UN on developments in the field of information and telecommunications of 2013 and 2015 are analysed. Also international agreements on international information security and OECD Recommendation on Digital security risk management for economic and social prosperity of 2015 are considered.

Keywords: *information security; international law; international organizations; Organisation for Economic Co-operation and Development; the United Nations*

Одним из ключевых институтов международного информационного права, активно развивающимся в последнее десятилетие, является институт международной информационной безопасности.

Формирование данного института осуществляется как на основе юридически обязательных норм международных договоров, так и из «мягкого права» - деклараций, рекомендаций и докладов органов международных организаций – таких как ООН, ОЭСР, ШОС, ОДКБ и др.

В настоящее время можно выделить две тенденции развития права международной информационной безопасности.

Первая, традиционная, основана на концепции угроз информационной безопасности, а также признания ключевой роли государств в регулировании данной сферы и многостороннего» *(англ. – multi-lateral)* регулирования (мультилатерализма). Данное направление развития осуществляется в рамках работы периодически формируемых групп правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также в рамках таких международных организаций, как ШОС и ОДКБ.

Вторая тенденция основывается на концепции управления рисками цифровой безопасности в рамках ОЭСР и так называемого много-субъектного регулирования *(англ. - multi-stakeholderregulation)*.

Концепцию «мультистейкхолдеризма» *(англ. – multistakeholderism)* следует определять именно как «много-субъектное регулирование» *(англ. – multi-stakeholderregulation)*. Ее ключевым отличием от мультилатерализма является включение в число субъектов-регуляторов не только государств, но и граждан, бизнеса и институтов гражданского общества. Следует отметить, что противостояние двух подходов – мультистейкхолдерной модели, основанной на участии всех заинтересованных сторон, и мультилатеральной, которая отдает приоритет международной дипломатии и международным организациям, было рассмотрено 7 апреля 2016 г. на 7 Российском форуме по управлению Интернетом. У. Дрейк (Университет Цюриха) высказал мнение, что две эти модели следует рассматривать не как взаимоисключающие, а как взаимодополняющие, а мультистейкхолдерной модели следует заимствовать у мультилатерализма более строгое следование законам и правилам[1].

В рамках ООН в 1998 г. по инициативе РФ была принята резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[2] (A/RES/53/70), предусматривающая подготовку докладов Генерального секретаря ООН по данной теме, содержащих позиции государств-членов ООН по таким вопросам, как:

– общая оценка проблем информационной безопасности;

– усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

– содержание концепций (информационная безопасность, несанкционированное вмешательство, неправомерное использование;

– возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне.

С 2010 г. Генеральным секретарем ООН представлялись доклады, содержащие позиции государств по вопросам информационной безопасности (2010 г. – A/65/154, 2011 г. – A/66/152, 2013 г. – A/68/156, 2014 – A/69/112).

Кроме того, в период 2004-2015 г.г. были созданы 4 группы правительственных экспертов, представлявшие свои доклады соответственно, на 60-й, 65-й, 68-й и 70-й сессиях Генеральной ассамблеи ООН.

В докладе, представленном на 68-й сессии Генеральной ассамблеи ООН в 2013 г., указано, что государственный суверенитет и международные нормы и принципы, вытекающие из принципа государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием ИКТ, а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории (п. 20)[3].

В докладе группы правительственных экспертов, представленной на 70-й сессии Генеральной ассамблеи ООН в 2015 г.[4], данная группа предлагает государствам рассмотреть следующие рекомендации в отношении добровольных и необязательных норм, правил или принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды:

а) в соответствии с целями Устава Органи-

зации Объединенных Наций, в том числе касающимися поддержания международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности;

б) в случае инцидентов в сфере ИКТ государства должны изучить всю соответствующую информацию, в том числе более общий контекст события, проблемы присвоения ответственности в ИКТ-среде, а также характер и масштабы последствий;

в) государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с использованием ИКТ;

г) государства должны рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также осуществлять другие совместные меры по противодействию таким угрозам. Государствам, возможно, потребуется рассмотреть вопрос о разработке новых мер в этой сфере;

д) в процессе обеспечения безопасного использования ИКТ государства должны соблюдать положения резолюций 20/8 и 26/13 Совета по правам человека о поощрении, защите и осуществлении прав человека в Интернете и резолюций 68/167 и 69/166 Генеральной Ассамблеи о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать свое мнение;

е) государство не должно осуществлять или заведомо поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит его обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения;

и) государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции;

к) государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ. Государства должны также удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере ИКТ, направленных против критически важной инфраструктуры других государств, если такие действия проистекают с их территории, принимая во внимание должным образом концепцию суверенитета;

л) государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование пагубных скрытых функций;

м) государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры;

н) государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группам готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности.

В отношении реализации государственного суверенитета в докладе отмечено, что суверенитет государств и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территориях.

Согласно позиции Министерства иностранных дел РФ, итоговый доклад Группы является важным политико-правовым документом, закладывающим общие рамки для взаимодействия государств в информационном пространстве[5].

Развитие международно-правового института международной информационной безопасности в форме международно-правовых договоров в настоящее время осуществляется только в рамках отдельных международных организаций либо на двухстороннем уровне.

Например, согласно Концепции сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, утв. Решением Совета глав государств Содружества Независимых Государств от 10 октября 2008 г.[6], интересы государств – участников СНГ в информационной сфере заключаются в ее гармоничном формировании, наиболее эффективном развитии и использовании в целях реализации прав и свобод человека и общества, соблюдения норм законности и правопорядка, *обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности государств – участников СНГ*, достижения ими экономического роста, политической и социальной стабильности.

16 июня 2009 г. было подписано межправительственное Соглашение между правительствами государств—членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, которое среди принципов закрепляет невмешательство в информационные ресурсы государств Сторон (статья 4). Каждая Сторона имеет равное право на защиту информационных ресурсов и критически важных структур своего государства от неправомерного использования и несанкционированного вмешательства, в том числе от информационных атак на них.

На уровне Российской Федерации в 2013 г. Президентом РФ были утверждены Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года[7].

Под международной информационной безопасностью в Основах понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

Под системой международной информационной безопасности понимается совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства.

Система международной информационной безопасности призвана оказать противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве.

Согласно Основам, цель государственной политики РФ заключается в содействии установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности.

Совет Безопасности РФ осуществляет мониторинг реализации Основ. В частности, 3 февраля 2016 г. в аппарате Совета Безопасности Российской Федерации подведены итоги деятельности органов государственной власти, направленной на содействие формированию системы международной информационной безопасности[8].

20 ноября 2013 г. подписано Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности[9]. Данное соглашение не содержит положений о суверенитете государств и связи суверенитета и информационной безопасности.

Советом безопасности РФ разработана концепция универсальной Конвенции об обеспечении международной информационной безопасности[10].

Согласно данной концепции, политические полномочия по связанным с Интернетом вопросам государственной политики являются суверенным правом государств, и что государства имеют права и обязанности в отношении связанных с Интернетом вопросов государственной политики международного уровня. Деятельность государств в информационном пространстве должна гарантировать свободу технологического обмена и сво-

боду обмена информацией с учетом уважения суверенитета государств и их существующих политических, исторических и культурных особенностей.

Согласно концепции, в целях создания и поддержания атмосферы доверия в информационном пространстве необходимо соблюдение государствами следующих принципов:

– деятельность каждого государства-участника в информационном пространстве должна способствовать социальному и экономическому развитию и осуществляться таким образом, чтобы быть совместимой с задачами поддержания международного мира и безопасности, соответствовать общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы в международных отношениях, невмешательства во внутренние дела других государств, уважения суверенитета государств, основных прав и свобод человека;

– все государства-участники в информационном пространстве пользуются суверенным равенством, имеют одинаковые права и обязанности и являются равноправными субъектами информационного пространства независимо от различий экономического, социального, политического или иного характера;

– каждое государство вправе устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством. Суверенитет и законы распространяются на информационную инфраструктуру, расположенную на территории государства-участника или иным образом находящуюся под его юрисдикцией. Государства должны стремиться к гармонизации национальных законодательств, различия в них не должны создавать барьеры на пути формирования надежной и безопасной информационной среды;

– каждое государство, учитывая законные интересы безопасности других государств, может свободно и самостоятельно определять свои интересы обеспечения информационной безопасности на основе суверенного равенства, а также свободно выбирать способы обеспечения собственной информационной безопасности в соответствии с международным правом.

Концепция Конвенции оказала значительное влияние на подписание двухсторонних соглашений РФ в сфере международной информационной безопасности.

11 июля 2014 г. было подписано межправительственное Соглашение между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности. Соглашение относит к числу основных угроз международной информационной безопасности неправомерное использование информационных и коммуникационных технологий:

– в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на нарушение суверенитета, территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

– для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей и теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию и нестабильности, а также для дестабилизации внутриполитической обстановки, нарушения управления государством и в целях свержения конституционного строя.

8 мая 2015 г. было подписано межправительственное Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности. Документ вступил в силу 10 августа 2016 г.

В преамбуле данного Соглашения подтверждается, что государственный суверенитет и международные нормы и принципы, вытекающие из государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием информационно-коммуникационных технологий, и юрисдикцию государств над информационной инфраструктурой на их территории, а также то, что государство имеет суверенное право определять и проводить государственную политику по вопросам, связанным с информационно-телекоммуникационной сетью «Интернет», включая обеспечение безопасности.

Согласно Соглашению, первой среди ос-

новных угроз международной информационной безопасности является использование информационно-коммуникационных технологий для осуществления актов агрессии, направленных на нарушение суверенитета, безопасности, территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

25 июня 2016 г. было подписано Совместное заявление Президента Российской Федерации и Председателя Китайской Народной Республики о взаимодействии в области развития информационного пространства[11]. Согласно данному заявлению, руководители двух стран поддерживают принцип уважения государственного суверенитета в информационном пространстве, рациональные требования всех стран по защите собственной безопасности и развитию, предлагают сформировать мирное, безопасное, открытое и основанное на сотрудничестве информационное пространство и разработать в рамках ООН универсальные правила ответственного поведения в информационном пространстве. Они выступают за равные права для всех государств на участие в управлении сетью Интернет, а также признают право на защиту национальной безопасности в информационном пространстве с учётом практики законодательства и государственной системы, поддерживают инициативу создания многосторонней, демократичной, прозрачной системы управления сетью Интернет и важную роль ООН в вопросе создания международных механизмов управления Интернетом.

Как было указано выше, одним из ключевых элементов реализации государственного суверенитета в информационной сфере является осуществление юрисдикции в отношении ИКТ-инфраструктуры на территории данного государства, а двухсторонние соглашения в сфере международной информационной безопасности содержат специальные нормы об информационной инфраструктуре и о критических важных объектах.

Вместе с тем, принимаемые в рамках международных организаций документы об обеспечении информационной безопасности в отношении информационной инфраструктуры, содержат разные понятия.

Вышеуказанные соглашения с Республикой Кубой 2014 г. и Китайской народной республикой 2015 г. определяют информационную инфраструктуру как совокупность технических средств и систем создания, преобразования, передачи, использования и хранения информации, Соглашение ШОС 2009 г. – как совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации.

Соглашение с Китайской народной республикой 2015 г. содержит также понятие «критически важные объекты» - объекты инфраструктуры государства, нарушение или прекращение функционирования которых приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению или разрушению экономики государства либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на территории государства, на длительный срок. Соглашение ШОС 2009 г. содержит иное понятие - «критически важные структуры» — объекты, системы и институты государства, воздействие на которые может иметь последствия, прямо затрагивающие национальную безопасность, включая безопасность личности, общества и государства.

В рамках работы Межпарламентской ассамблеи СНГ 28 ноября 2014 г. приняты модельные законы «Об информации, информатизации и обеспечении информационной безопасности»[12] и «О критически важных объектах информационно-коммуникационной инфраструктуры»[13].

Модельный закон «Об информации, информатизации и обеспечении информационной безопасности» содержит понятие критически важная информационно-коммуникационная инфраструктура – совокупность средств и систем формирования, создания, преобразования, передачи, использования и хранения информации, отказ или разрушение которых может оказать существенное отрицательное воздействие на национальную безопасность.

В свою очередь, модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры» содержит иные понятия:

информационно-коммуникационная инфраструктура – совокупность территориально распределенных государственных и корпоративных информационных систем, сетей связи, средств коммутации и управления информационными потоками, а также орга-

низационных структур и нормативно-правовых механизмов регулирования, обеспечивающих их эффективное функционирование;

критически-важные инфраструктуры – объекты, системы, службы и институты, разрушение или выведение из строя которых может нанести серьезный ущерб социальному, экономическому или политическому порядку или национальной безопасности;

критический элемент критически важного объекта информационно-коммуникационной инфраструктуры – структурный компонент критически важного объекта информационно-коммуникационной инфраструктуры, выход из строя которого с неизбежностью приводит к нарушению или прекращению функционирования объекта в целом;

объект информационно-коммуникационной инфраструктуры – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения функционирования такого объекта, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, а также персонала, который осуществляет их эксплуатацию.

В рамках Парламентской Ассамблеи Организации Договора о коллективной безопасности также принят рад документов, содержащих различные понятия и их определения:

– Рекомендации по гармонизации законодательства государств- членов ОДКБ в сфере обеспечения безопасности критически важных объектов от 27 ноября 2014 г. №7-5[14];

– Рекомендации по сближению и гармонизации национального законодательства государств - членов ОДКБ в сфере обеспечения информационно - коммуникационной безопасности от 27 ноября 2014 г. №7-6[15].

Параллельно с процессами развития института международной информационной безопасности под эгидой ООН, идет формирование института регулирования цифровой экономики и цифровой безопасности в рамках ОЭСР.

17 сентября 2015 г. Совет ОЭСР принял Рекомендацию и сопроводительный документ по управлению рисками цифровой безопасности для экономического и социального процветания (Digitalsecurityriskmanagementforeconomicandsocialprosperity.OECD Recommendation and Companion Document. 17 September 2015 – C (2015) 115)[16].

Нацеливая государства на принятие стратегий цифровой безопасности, данная Рекомендация не содержит упоминаний о суверенитете государств в цифровом пространстве. Однако при этом неоднократно подчеркивается значимость вовлечения всех заинтересованных субъектов *(англ. - allstakeholders),* т.е. Рекомендация ориентирована на так называемое много-субъектное регулирование *(англ. - multi-stakeholderregulation)*.

Таким образом, анализ тенденций развития института международной информационной безопасности как элемента реализации государственного суверенитета, позволяет сделать следующие выводы:

– формирование подходов к регулированию международной информационной безопасности на универсальном уровне идет в рамках рекомендаций группы правительственных экспертов ООН, носящих характер «мягкого права»;

– развитие российской модели международной информационной безопасности осуществляется в рамках двухсторонних соглашений, которые в перспективе смогут являться основой для подписания многосторонних конвенций как на региональном уровне, так и в рамках ООН;

– необходима координация действий в рамках различных международных организаций, направленная на формирование и обеспечение единого международно-правового режима информационной безопасности на основе единого понятийного аппарата и принципов;

– параллельно с развитием института международной информационной безопасности осуществляется формирование института управления рисками цифровой безопасности при построении так называемой цифровой экономики. Данный институт, в отличие от международной информационной безопасности, ориентирован в значительной мере не на участие государств, а на «многосубъектное» регулирование.

Примечания

1. Разные модели управления интернетом дополняют друг друга // Координационный центр национального домена сети Интернет. URLhttps://cctld.ru/ru/press_center/news/news_detail.php?ID=9661 (дата обращения 02.09.2016)

2. Официальный сайт ООН. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения 02.09.2016)

3. Доклад Группы правительственных экспертов по достижениям в сфере информатизациии телекоммуникаций в контексте международной безопасности. A/68/98. Официальный сайт ООН. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R (дата обращения 02.09.2016)

4. Доклад Группы правительственных экспертов по достижениям в сфере информатизациии телекоммуникаций в контексте международной безопасности. A/70/174. Официальный сайт ООН. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement (дата обращения 02.09.2016)

5. Об итогах заключительного заседания Группы правительственных экспертов ООН по международной информационной безопасности. Официальный сайт МД России. URL: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/1525144 (дата обращения 02.09.2016)

6. Интернет-портал СНГ. URL: http://www.e-cis.info/page.php?id=20229 (дата обращения 02.09.2016)

7. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утверждены Президентом РФ 24 июля 2013 г., № Пр-1753 // СПС «Консультант Плюс»

8. Совет Безопасности Российской Федерации. Официальный сайт. URL: http://www.scrf.gov.ru/news/1020.html (дата обращения 02.09.2016)

9. Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001201506040007 (дата обращения 02.09.2016)

10. Конвенция об обеспечении международной информационной безопасности (концепция) // Совет Безопасности Российской Федерации. Официальный сайт. URL: http://www.scrf.gov.ru/documents/6/112.html (дата обращения 02.09.2016)

11. Совместное заявление Президента Российской Федерации и Председателя Китайской Народной Республики о взаимодействии в области развития информационного пространства от 25 июня 2016 г. // Президент России. Официальный сайт. URL: http://www.kremlin.ru/supplement/5099 (дата обращения 02.09.2016)

12. Документы Межпарламентской Ассамблеи Содружества независимых государств. URL: http://iacis.ru/upload/iblock/25c/prilozhenie_k_postanovleniyu_15.pdf (дата обращения 02.09.2016)

13. Документы Межпарламентской Ассамблеи Содружества независимых государств. URL: http://iacis.ru/upload/iblock/f3b/prilozhenie_k_postanovleniyu_14.pdf (дата обращения 02.09.2016)

14. Парламентская Ассамблея Организации Договора о коллективной безопасности. URL: http://www.paodkb.ru/upload/iblock/917/rekomendatsii-po-garmonizatsii-zak_va-gos._chlenov-odkb-v-sfere-obespech.-bezop.-kritich.-vazhn.-obektov.pdf (дата обращения 02.09.2016)

15. Парламентская Ассамблея Организации Договора о коллективной безопасности. URL: http://www.paodkb.ru/upload/iblock/c07/rekomendatsii-po-sblizhen.-i-garmoniz.-natsion.-zak_va-gos._chlenov-odkb-v-sfere-obesp.-inf._kommunik.-bezop..pdf (дата обращения 02.09.2016)

16. OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, 2015. 74 p.

ЕФРЕМОВ Алексей Александрович, ведущий научный сотрудник Центра технологий государственного управления ИПЭИ РАНХиГС, кандидат юридических наук, доцент. 119571, г. Москва, проспект Вернадского, д. 82. E-mail: efremov-a@ranepa.ru

YEFREMOV Alexey, Senior Researcher of the Center for Public Administration Technologies in RANEPA Institute of Applied Economic Research, Candidate of Law, Associate Professor. Vernadskogo Prospect 82, Moscow, 11957, Russia. E-mail: efremov-a@ranepa.ru

Вестник УрФО № 1(23) / 2017, с. 40–43
УДК - 004.056.53 + 351.865:004.056 + 341.1:004.056

Мальцева М.Д.

ИМПОРТОЗАМЕЩЕНИЕ КАК АСПЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье проводится анализ вопросов национальной информационной безопасности, обеспечиваемой с помощью системы импортозамещения. Также анализируются нормативные акты, которыми такое импортозамещение предусмотрено. Производится сравнение практики импортозамещения информационной продукции в России и за рубежом. Делается вывод, что введенная в России система импортозамещения программного обеспечения является разрешительной и имеет сходства с реагированием импортозамещения в Китае. Указывается, что импортозамещение возможно только в случае, если отечественные производители теоретически и практически способны обеспечить надлежащее удовлетворение потребностей потребителей в информационных услугах и продукции.

Ключевые слова: *импортозамещение, информационная безопасность Российской Федерации, программное обеспечение, информационный суверенитет государства.*

Maltseva M. D.

IMPORT SUBSTITUTION IS A CONSIDERATION FOR INFORMATION SECURITY

The article analyses the issues of national information security provided by import substitution system. The article as well analyses legal regulation of import substitution. Practices of import substitution of information goods in Russia and abroad are compared. It is concluded that put in force import substitution in Russia resembles legal regulation of import substitution in China. It is pointed out that import substitution is applicable only in case when domestic producers are theoretically and practically able to provide for due satisfaction of consumers' needs in informational services and goods.

Keywords: *import substitution, information security of Russian Federation, software, information national sovereignty*

Национальная безопасность России во многом зависит от обеспечения защищенности информационной сферы общества в рамках государства. При этом роль обеспечения информационной безопасности с учетом технического прогресса и глобализации, которая не только открывает новые возможности, но и создает определенные риски, будет возрастать. В то время как сложившаяся геополитическая ситуация выявила значительную зависимость российских потребителей от информационных продуктов, производимых за

рубежом, кибертерроризм, кибершпионаж, таргетированные атаки на инфраструктуру компаний и госструктур повлияли на принятие на законодательном уровне нормативных актов, касающихся импортозамещения в информационной сфере.

Концептуальным документом, определяющим государственную политику в сфере информационной безопасности, является Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 09.09.2000 г. № Пр-1895[1], согласно которой под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В практической сфере под информационной безопасностью понимают охрану каналов поступления, хранения, обработки и передачи информации, защита любых информационных ресурсов по уровням доступа[2]. При этом такая безопасность может обеспечиваться как при помощи технических мер, так и при помощи организационных мер, среди которых существенное значение имеет импортозамещение иностранных программных продуктов.

Несмотря на то, что в данной Доктрине понятие «импортозамещение» не упоминается, отдельные положения свидетельствуют о том, что приоритетным направлением государственной политики в информационной сфере является поддержка отечественных производителей продукции и услуг в сфере информационных и телекоммуникационных технологий, а также предотвращение угроз национальной безопасности. Вместе с тем именно на защиту от несанкционированного доступа к обрабатываемой информации и уменьшение зависимости России от иностранных производителей компьютерной, телекоммуникационной техники и программного обеспечения направлено импортозамещение.

Другим нормативным актом, указывающим на необходимость импортозамещения, является Стратегия развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года, утвержденной Распоряжением Правительства РФ от 01.11.2013 г. № 2036-р[3], которой предусмотрена разработка и запуск специальной программы импортозамещения продукции сферы информационных технологий для решения задач отдельных государственных структур и организаций (в том числе оборонно-промышленного комплекса), а также ряд иных мер, направленных на обеспечение информационной безопасности, таких как: стимулирование циркуляции данных «облачных» сервисов внутри страны, обеспечение стабильности развития отечественной отрасли информационных технологий и ее суверенности в долгосрочной перспективе за счет создания условий для развития в стране глобальных лидеров.

Ограничение закупок иностранного программного обеспечения государственными и муниципальными заказчиками было введено Постановлением Правительства Российской Федерации от 16.11.2015 г. №1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»[4].

Практика импортозамщения информационной продукции широко применятся по всему миру. Так в США существует несколько нормативных актов в сфере импортозамещения. В частности, Положение о предпочтении американских товаров при осуществлении правительственных закупок (Buy American Act) предоставляет преференции национальным производителям и разработчикам, в то время как Закон о торговых соглашениях (Trade Agreements Act) устанавливает запрет на закупки для государственных нужд продуктов, произведенные в третьих странах, при этом для некоторых стран предоставляется национальный режим США. В Китае государственные закупки товаров и услуг, в том числе в сфере информационных технологий, ограничены реестром, который содержит наименования «разрешенных» продуктов. Критерии для внесения продукта в список, устанавливаются на подзаконном уровне уполномоченными органами. В ЕС действует принцип недискриминации иностранных компаний, в то же время ведется работа по ограничению доступа компаний из стран, не являющихся участницами ЕС, к процессу государственных закупок[5].

Система импортозамещения программного обеспечения, введенная в России, имеет сходства с указанной выше китайской разрешительной системой. Федеральным законом

от 29.06.2015 г. № 188-ФЗ[6] предусмотрено создание единого реестра российских программ для электронных вычислительных машин и баз данных в целях расширения использования российского программного обеспечения и подтверждения его российского происхождения. Не смотря на это относительно недавнее нововведение, в данном реестре на 20.02.2016 г. находятся 87 позиций, среди которых представлены следующие классы программных продуктов: операционные системы, системы управления процессами организации, системы управления базами данных, средства обеспечения облачных и распределительных вычислений, средства виртуализации и системы хранения данных, серверное и связующее ПО, поисковые системы, системы мониторинга и управления, средства обеспечения информационной безопасности, офисные приложения, системы сбора, хранения, обработки, анализа, моделирования и визуализации массивов данных, системы управления проектами, исследованиями, разработкой, проектированием и внедрением, а также лингвистическое программное обеспечение[7].

Из указанного выше Постановления Правительства РФ следует, что исключение при осуществлении госзакупок составляют случаи, когда программное обеспечение с необходимыми функциональными, техническими и (или) эксплуатационными характеристиками в России отсутствует.

В рассматриваемом контексте следует учитывать структуру информационной безопасности, состоящую из трех основных элементов: состояние информационной среды, обеспечивающее удовлетворение информационных потребностей субъектов информационных отношений; безопасность информации; защищенность субъектов от негативного информационного воздействия[8].

Следовательно, политика импортозамещения должна быть направлена не только на безопасность информации, но и на обеспечение такой информационной среды, при которой было бы возможным удовлетворение потребностей государственных и муниципальных структур. Данное обстоятельство указывает на то, что возможность импортозамещения информационной продукции неразрывно связана с производством аналогичной продукции отечественными компаниями. В связи с этим особое внимание должно быть уделено стимулированию деятельности отечественных разработчиков, работающих в области информационных технологий. Так, для ИТ-компаний предусмотрены льготные ставки тарифов страховых взносов, упрощенный порядок привлечения высококвалифицированных иностранных специалистов, а также некоторые налоговые льготы (освобождение от НДС, льготная амортизация).

Таким образом, необходимость соблюдения государственных интересов в информационной сфере послужила причиной использования такого экономического средства политики национальной безопасности как импортозамещение, которое, в свою очередь, призвано послужить одной из основ для построения информационного суверенитета Российской Федерации.

Примечания

1. Доктрина информационной безопасности Российской Федерации: утв. Президентом Российской Федерации 09.09.2000 г. № Пр-1895 // СПС «Консультант плюс».

2. Мигачев Ю.И., Молчанов Н.А. Правовые основы национальной безопасности (административные и информационные аспекты) // Административное право и процесс. 2014. - № 1. - с. 46.

3. Распоряжение Правительства РФ от 01.11.2013 г. № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года» // СПС «Консультант плюс».

4. Постановление Правительства Российской Федерации от 16.11.2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» // СПС «Консультант плюс».

5. Мелащенко Н.В., Наумов В.Б. Подходы к правовому регулированию импортозамещения в сфере информационных технологий в США, КНР, ЕС и России // Инновации. 2015. - № 6. – с.16 -18.

6. Федеральный закон от 29.06.2015 г. № 188-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статью 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // СПС «Консультант плюс».

7. В реестр российского программного обеспечения добавлено 84 продукта// Официальный интернет-ресурс Минкомсвязи России. URL: http://www.minsvyaz.ru/ru/events/34715/ (дата обращения: 24.02.2016).

8. Яковец Е.Н. Правовые основы обеспечения информационной безопасности Российской Федерации: учебное пособие. М.: Юрлитинформ, 2014. с. 408.

МАЛЬЦЕВА Мария Дмитриевна, аспирантка кафедры теории государства и права, конституционного и административного права Южно-Уральского государственного университета. 454080, г. Челябинск, пр. Ленина, 76. E-mail: mmd812@mail.ru

Maltseva Maria, graduate student of Theory of state and law, constitutional and administrative law of the South Ural State University. 454080, Chelyabinsk, Lenina ave., 76. E-mail: mmd812@mail.ru

УДК - 343.13:004 + 343.9.01 Вестник УрФО № 1(23) / 2017, с. 44–47

Соколов Ю.Н.

ПРИРОДА УГОЛОВНО-ПРОЦЕССУАЛЬНОЙ ИНФОРМАЦИИ И ЕЕ ОСОБЕННОСТИ

Основываясь на категориальной модели информации[1] и выполнив анализ элементов информационного взаимодействия человека с окружающей его действительностью, автором рассмотрены особенности уголовно-процессуальной информации, акцентировано внимание на ее специфике обусловленной сферой уголовного судопроизводства. В предложенной структурной модели, учтены и такие, достаточно сложные ее формы, как электронная информация.

Основываясь на нормах права действующего законодательства, выделены основные виды закрепления и фиксации уголовно-процессуальной информации с учетом современных информационных технологий.

Дается авторское понятие базовой категории уголовного судопроизводства, излагаются рекомендации по внесению изменений в действующий уголовно-процессуальный закон с целью однозначного толкования и возможности конструирования отдельных норм права составляющих отдельные институты доказательственного права.

Ключевые слова: информация, преступление, уголовный процесс, протокол, уголовно-процессуальная информация.

Sokolov Yu. N.

THE NATURE OF THE CRIMINAL-PROCEDURAL INFORMATION AND FEATURES

Based on categorical model information and performing analysis of the elements of human information interaction with the surrounding reality, the author describes the features of criminal procedure information, focusing on the specifics of its due sphere of criminal proceedings. The proposed structural model, accounted for and are sufficiently complex forms as electronic information.

Based on the rules of law applicable legislation, identified the main types of fastening and fixing of criminal procedure information based on modern information technologies.

The author's concept of the basic categories of criminal proceedings, sets out the recommendations for amendments to the current criminal procedure law to unambiguous interpretation and the possibility of designing the individual components of the law of evidence separate institutions.

Keywords: information, crime, criminal procedure, protocol, criminal procedure information.

Информация как категория – это абстрактная модель существующей действительности, отдельных моментов бытия, в т.ч. связанных с событием преступления, его расследованием, собиранием информации, имеющей отношение к уголовному делу, формированием доказательств, всей уголовно-процессуальной действительности.

Предлагаемая категориальная модель информации характеризует ее природу и дает ответ на вопрос, что представляет собой ее сущность.

Категории, будучи предельно общим фундаментальным понятием, отражают наиболее существенные связи реальной действительности, они представляют собой наиболее глубокие по содержанию и широкие по объему понятия[2].

Поэтому информация как абстрактная модель всегда соотносится с конкретным видом информации, как более уточненным образом окружающей нас действительности. Чтобы понять особенности исследуемого объекта необходимо остановиться на его специфике обусловленной сферой уголовного судопроизводства. Для этого целесообразно взять за основу компоненты информационного взаимодействия человека, выделенные Н. Винером[3] и рассмотрим аналогичные элементы в сфере уголовного процесса.

Уголовно-процессуальная информация представляет собой образ события преступления (время, место, способ и другие события совершения преступления) как явления социальной действительности. Преступление как виновно совершенно общественно опасное деяние, запрещенное уголовным законом, характерно только для социальной действительности, связанной с жизнью в соответствующем обществе, отношениями в обществе или к обществу. В нашем случае, уголовно-процессуальная информация как категории уголовного процесса, выступает отдельным видом по отношению к информации в целом, а значит и соответствующей сферой бытия.

Образ события преступления отражается в сознании участников уголовного судопроизводства. Изначально, анализируемый образ может быть отражен в сознании неопределенного (неустановленного) круга лиц, однако для уголовно-процессуальной информации присуще формально определенная группа субъектов, закрепленная уголовно-процессуальным законом. Прежде чем любая информация имеющая отношение для уголовного дела получит соответствующий статус, она должна быть собрана, закреплена, проверена и оценена в результате проведения следственных и иных процессуальных действий, причем активными действиями со стороны участников уголовного процесса.

Несомненно, событие преступления оставляет не только идеальные следы в сознании людей, но и материальные, виртуальные следы, являющиеся объективной и ретроспективной информацией по своей сути. Возникшие образы в данном случае присутствуют на объектах неорганического и органического мира, в электронной среде источников (носителей) информации, но не является еще уголовно-процессуальной информацией. Как мы уже отметили выше, данные образы должны первично отразиться в сознании рассмотренных участников. Установленная специфика, выступает особенностью уголовно-процессуальной информации наряду с ее ретроспективностью.

Виртуальные образы еще характерны тем, что они обусловлены электронной (искусственной) средой своего существования созданной и поддерживаемой человеком. Названные образы создаются в электромагнитной среде своего существования и хранятся во внутренней памяти (оперативной или постоянной) электронного источника (носителя) информации. Так криминалисты предлагают понимать под виртуальным следом зафиксированный компьютерной системой на цифровом материальном носителе результат отражения реального (физического) процесса или действия иной компьютерной системы, связанный с преступлением (имеющий уголовно-релевантное значение), в виде цифрового образа формальной модели этого процесса[4].

Тем не менее, ранее предложенная структурная модель природы информации учитывает и такие, достаточно сложные ее формы, как электронная информация.

Уголовно-процессуальная информация в соответствии с требованиями уголовно-процессуального закона закрепляется в письменной протокольной форме, электронной или иной документальной форме. Протокол – официальный документ, содержащий запись всего, что было сказано, сделано и решено[5].

В ст. 1 Федерального закона от 29 января 1994 г. № 77-ФЗ «Об обязательном экземпля-

ре документов»[6] и ст. 1 Федерального закона от 29 декабря 1994 г. № 78-ФЗ «О библиотечном деле»[7], законодатель под документом понимает «… материальный носитель с зафиксированной на нем информацией в виде текста, звукозаписи (фонограммы), изображения или их сочетания, предназначенный для передачи во времени и пространстве в целях общественного использования и хранения».

Документировать - обосновывать документами[8].

В ст. 2 Федерального закона «Об информации, информационных технологиях и защите информации», под документированной информацией (документом) понимается - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее носитель[9].

Уголовно-процессуальный закон содержит общие правила производства следственных действий[10], определяет форму и содержание протокола следственного действия[11], регламентирует порядок производства каждого из них[12]. В УПК РФ также закреплен порядок ведения, форма и содержание протокола судебного заседания[13] и процедура судебных действий, проводимых в судебном следствии[14].

При производстве следственных и судебных действий могут применяться альтернативные средства фиксации информации: фотосъемка, видеозапись, электронный протокол судебного заседания и др.[15] Данные средства и являются основными источниками электронной формы информации.

Еще одним компонентом информационного взаимодействия человека с действительностью выступает цель такого взаимодействия.

По мнению М.И. Сетрова, сообщение для каждой категории людей несет совершенно разную информацию, соответствующую кругу интересов получателя.

Таким образом, одно и то же сообщение, по-разному интерпретированное, может нести разную информацию. При этом можно утверждать, что «решающим для связи между сообщением и содержащейся в нем информации является некоторое отображение, которое является либо результатом договоренности, либо результатом понимания, либо предписанным правилом. Это отображение можно обозначить, как правило, интерпретации[16]».

Заметим, что некоторое правило интерпретации для отдельного сообщения чаще всего являются частным случаем более общего правила, применимого к определенному множеству сообщений, если они в свою очередь построены по одинаковым законам.

Однако знание только правил интерпретации совсем не достаточно для извлечения информации из сообщения. Сама интерпретация определяется интересами получателя информации, его чувствами, эмоциями и, говоря более формальным языком, - просто его целью.

При этом несложно представить, что одним из основных условий извлечения необходимой информации из сообщения является собственно цель этого процесса.

В качестве цели уголовного судопроизводства следует назвать защиту человека, общества и государства от преступной деятельности, а такая защита в полной мере может быть осуществлена, когда имеется истинное представление (понимание) его ретроспективной картины.

Учитывая вышеизложенное, можно предложить следующее понятие уголовно-процессуальной информации. Это образ события преступления как явления социальной действительности, отраженный в сознании участников уголовного судопроизводства и закрепленный в письменной, электронной или иной документальной форме допустимой уголовно-процессуальным законом, с целью получения истинного представления (понимания) его ретроспективной картины.

Полагаем, что для единообразного толкования закона предлагаемое понятие может быть закреплено в ст. 5 УПК РФ. Это позволит ввести в научный и практический оборот одну из базовых категорий уголовного процесса в сферу уголовного судопроизводства, обеспечит ее однозначное понимание и возможность конструирования отдельных норм права составляющих отдельные институты доказательственного права, таких как: собирание доказательств, их проверку, оценку и использование; сущность доказательств и их виды[17].

Примечания

1. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / под ред. В.А. Садовничего, В.П. Шерстюка. М.: МЦНМО, 2002. С. 21-39; Кузнецов П.У. Информационные основания права: монография. Екатеринбург: Издательский дом «Уральская государственная юридическая академия», 2005. С. 65.

2. Ивин А.А. Никифоров А.Л. Словарь по логике. М., 1997. С. 142; Васильев А.М. Правовые категории. Методологические аспекты разработки системы категорий теории права. М., 1976. С. 58.

3. Винер Н. Кибернетика и общество. / Пер. Е.Г. Панфилова. М.: Иностранная литература, 1958. С. 31.

4. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: Автореф. дисс. … канд. юрид. наук. Воронеж, 2010. С. 7.

5. Большой словарь иностранных слов. Издательство «ИДДК». 2007. С. 736.

6. Российская газета. 1995. 17 января.

7. Собрание законодательства Российской Федерации. 1995. № 1. Ст. 2.

8. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка. М.: А ТЕМП, 1999. С. 158.

9. Российская газета. 2006. 29 июля.

10. См.: ст. ст. 164, 165, 167-170 УПК РФ.

11. См.: ст. 166 УПК РФ.

12. См.: главы 24-27 УПК РФ.

13. См.: ст. 259 УПК РФ.

14. См.: ст. ст. 273-291 УПК РФ.

15. См.: ч. 5, 8 ст. 166, ч. 5 ст. 259 УПК РФ и др.

16. Сетров М.И. Информационные процессы в биологических системах. Л.: Наука, 1975. С.33.

17. Кузнецов Н.П. Уголовно-процессуальное доказывание и доказательственное право // Кокорев Л.Д., Кузнецов Н.П. Уголовный процесс: доказательства и доказывание. Воронеж, 1995. С. 12-13.

СОКОЛОВ ЮРИЙ НИКОЛАЕВИЧ, доцент кафедры информационного права Уральского государственного юридического университета, кандидат юридических наук, доцент. Россия, 620137, г. Екатеринбург, ул. Комсомольская, 21. E-mail: ur-sokol@rambler.ru.

SOKOLOV Yuri, Associate Professor of Information Law, Ural State Law University, Candidate of Legal Sciences, Associate Professor. Russia, 620137, Yekaterinburg, ul. Komsomolskaya, 21. E-mail: ur-sokol@rambler.ru.

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 (см. стр. 58) или заключение от экспертной комиссии (см. стр. 59)).

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.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ

УТВЕРЖДАЮ
Должность руководителя
организации или лица с
соответствующими полномочиями
_____И. О. Фамилия
«___»_____2015 г.

ЗАКЛЮЧЕНИЕ № _____

о возможности открытого опубликования

_____
(наименование материалов, подлежащих экспертизе)

Экспертная комиссия в составе _____

в период с «___»_____20___г. по «___»_____20___г. провела экспертизу материалов

_____
(наименование материалов, подлежащих экспертизе)

на предмет отсутствия (наличия) в них сведений, составляющих государственную тайну, и сведений, подпадающих под действие законодательства об экспортном контроле, и возможности (невозможности) их открытого опубликования.

Руководствуясь Законом Российской Федерации «О государственной тайне», Перечнем сведений, отнесенных к государственной тайне, утвержденным Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, а также Перечнем сведений, подлежащих засекречиванию Министерства образования и науки РФ, утвержденным приказом Минобрнауки РФ № 36с от 10.11.2014 г., а также Федеральным законом «Об экспертном контроле» от 18.07.1999 г. № 183-ФЗ и Указами Президента РФ № 1661 от 17.12.2011г, № 1005 от 08.08.2001 г., № 36 от 14.01.2003 г., № 202 от 14.02.1996 г., № 1083 от 20.08.2007 г., № 1082 от 28.08.2001 г., экспертная комиссия установила:

1) Сведения, содержащиеся в рассматриваемых материалах, находятся в компетенции *Наименование организации.*

2) Сведения, содержащиеся в рассматриваемых материалах, _____

_____
(указываются сведения, содержащиеся в материалах)

не подпадают под действие Перечня сведений, составляющих государственную тайну (статья 5 Закона Российской Федерации «О государственной тайне»), не относятся к Перечню сведений, отнесенных к государственной тайне, утвержденному Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, не подлежат засекречиванию, не подпадают под действие законодательства об экспортном контроле и данные материалы могут быть открыто опубликованы.

Председатель комиссии (Ф.И.О., подпись)

Члены ЭК : (Ф.И.О., подпись)

Секретарь ЭК (Ф.И.О., подпись)

ВЕСТНИК УрФО
Безопасность в информационной сфере № 1(23) / 2017

Дата выхода в свет 30.03.2017. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 5,25. Тираж 100 экз. Заказ 470/486.
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. 1(23) / 2017

Date of publication of the 30.03.2017. Format 70×108 1/16. Screen printing.
Conventional printed sheet 5,25. Circulation – 100 issues. Order 470/486. Open price.

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