УДК 004.056
DOI: 10.33764/2618-981X-2019-6-1-203-208

# ОЦЕНКА СООТВЕТСТВИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУРАХ РОССИЙСКОЙ ФЕДЕРАЦИИ

***Юлия Алексеевна Исаева***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (913)980-23-09, e-mail: Isaeva.JA@hotmail.com

***Валентин Валерьевич Селифанов***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (923)247-25-81, e-mail: sfo1@mail.ru

Продемонстрирована необходимость проведения оценки соответствия для средств защиты информации на значимых объектах критических информационных инфраструктур. При отсутствии описания необходимых критериев для информационных систем появляется возможность реализации угроз, что приведет к нарушению функционирования значимых объектов.

**Ключевые слова**: оценка соответствия, значимый объект, критическая информационная инфраструктура, безопасность информации.

# CONFORMITY ASSESSMENT OF INFORMATION PROTECTION TOOLS IN CRITICAL INFORMATION INFRASTRUCTURES OF THE RUSSIAN FEDERATION

***Julia A. Isaeva***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone: (913)980-23-09, e-mail: Isaeva.JA@hotmail.com

***Valentin V. Selifanov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (923)247-25-81, e-mail: sfo1@mail.ru

The need for conformity assessment of information security tools at significant objects of critical information infrastructures is demonstrated. In the absence of necessary criteria description for information systems, a possibility of threats implementation appears, which will lead to disruption of functioning of significant objects.

**Key words:** conformity assessment, significant object, critical information infrastructure, information security.

## *Введение*

Появление новых федеральных законов, приказов и постановлений Правительства связано с развитием информационных систем и технологий.

С вступлением в силу в 2018 г. Федерального закона Российской Федерации № 187 «О безопасности критической информационной инфраструктуры

Российской Федерации» [1] появился новый сегмент информационных систем, в которых требуется жесткое обеспечение информационной безопасности.

Рассматриваемый сегмент объединяет в себе достаточно большое количество разнородных объектов, которые делятся на три группы:

– информационные системы;

– автоматизированные системы управления технологическими процессами;

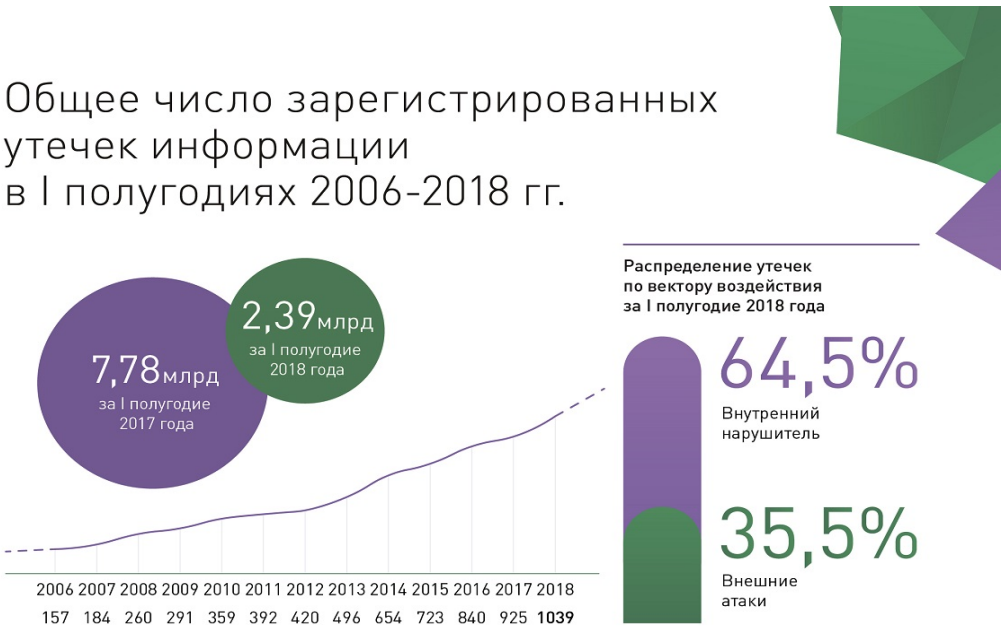
– информационно-телекоммуникационные сети.

Требования к безопасности, описанные в законе Российской Федерации № 187 [1], не обеспечивают достаточной защиты информации значимых объектов критической информационной инфраструктуры (далее ЗОКИИ), так как не описывают конкретных критериев, которым должны соответствовать информационная система и средства защиты информации. Действие требований распространяется на информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, которые отнесены к значимым объектам критической информационной инфраструктуры [3].

Необходимость защиты информации на ЗОКИИ обусловлена высоким риском появления чрезвычайных ситуаций при сбое системы, который может повлечь за собой угрозу жизни людей и огромный вред окружающей среде.

По статистике, основную опасность нарушения безопасности представляют собой внутренние нарушители. Так, утечки конфиденциальной информации представляют собой большую часть нарушений безопасности. По данным исследования компании InfoWatch, основными каналами утечек в 2016 г. стала сеть (браузер) и бумажная документация – на них приходится 64 и 26 % случаев соответственно [2]. Использование сети предполагает использование настольных версий мессенджеров, таких как What`sApp, Telegram, Viber и т. д. Две трети утечек в России происходит по вине сотрудников организации, которые имеют доступ к конфиденциальным данным. То есть утечка данных происходит от лиц, работающих в организации. Данная проблема касается различных учреждений. По числу утечек данных в России лидируют госорганы (21,6 %), высокотехнологичные компании (14,65 %), образовательные учреждения (13,6 %) и банки (11,75 %) [2]. В 2017 г. Аналитический центр InfoWatch зарегистрировал 254 случая утечки конфиденциальной информации из организаций, работающих в России. В результате скомпрометировано 5,8 млн записей, относящихся к персональным данным и финансовым данным, а также к другим типам конфиденциальной информации [4]. По данным исследования можно сказать, что утечек из-за внутренних нарушителей в два раза больше, чем утечек из-за внешних атак. На рисунке представлен график результатов исследований за двенадцать лет от компании InfoWatch [6]. Классический пример «медицинской утечки» – это «слив» сотрудниками учреждений здравоохранения данных о тяжелобольных пациентах ритуальным агентам [7].

Для предотвращения утечек конфиденциальных данных необходимо принимать срочные и жесткие меры.




Процентное соотношение внешних и внутренних нарушителей

Одним из решений проблемы утечки информации может являться приобретение и внедрение в информационные системы организаций, в том числе на ЗОКИИ, таких систем, как Data Loss Prevention (далее DLP). Данное средство защиты информации представляет собой систему для предотвращения утечек конфиденциальной информации.

Однако даже при выборе данного средства существует некоторое затруднение. Общие требования к обеспечению безопасности ЗОКИИ представлены в приказе ФСТЭК России № 239, однако, там указаны только общие аспекты обеспечения безопасности средствами защиты информации, и не регламентируется настройка функций безопасности в различных видах средств защиты.

### *Цель и задачи*

Таким образом, для обеспечения безопасности необходимо, чтобы предприятия, относящиеся к ЗОКИИ, имели единый регламент для установки и настройки средств защиты безопасности. При этом сохраняется возможность адаптированной настройки средств защиты, подходящей для определенных подсистем безопасности.

Этим регламентом является оценка соответствия средств защиты информации. Оценка соответствия – это прямое или косвенное определение соблюдения требований, предъявляемых к объекту оценки, в данном случае, к средству защиты информации. После проведения оценки можно будет утверждать, что средство защиты соответствует требованиям обеспечения безопасности. Помимо этого, проведение оценки соответствия по единому стандарту гарантирует необходимый уровень защиты информации предприятия. Для обеспечения на-

дежной защиты необходимо решить целый комплекс технических и организационных проблем с разработкой соответствующей документации [8].

Для реализации процесса оценки соответствия необходимо провести анализ известных решений на базе нормативных правовых актов, где присутствуют критерии выбора требований для проведения оценки. Так как DLP-системы являются средствами защиты информации, необходимо провести анализ методик проведения оценки соответствия DLP-систем в различных информационных системах.

Помимо анализа нормативной правовой базы, важным является и описание информационной системы. Инфраструктура системы безопасности является важным аспектом при внедрении средства защиты информации, а также при настройке правил безопасности и реагирования на инциденты безопасности.

После того, как будет составлено полное описание инфраструктуры системы безопасности, можно начинать разработку методик оценки соответствия DLP-систем. Для разработки методики необходимо учитывать инфраструктуру предприятия, но для того, чтобы методика подходила под различные средства защиты информации, должен существовать базовый набор критериев системы безопасности.

Когда программа и методики будут разработаны, необходимым условием принятия этих методик, как нормативного правового документа, является апробация. В том случае, если разработанная методика пройдет проверку работоспособности в реальных условиях, можно будет применять ее к различным информационным системам.

## *Методы и методики*

В данном исследовании средством защиты информации является DLP-система, и важным аспектом разработки методики оценки соответствия являются правила безопасности, при которых система будет реагировать на инциденты безопасности. Правила безопасности также должны быть включены в методику, как базовый набор правил. Это позволит системе безопасности установить необходимый уровень безопасности информационной системы и инфраструктуры в целом. Адаптивный набор правил будет возможно применять к DLP-системе для уточнения мер безопасности [5].

Зачастую угроза безопасности информации является следствием слабого места в информационной системе [9].

Во время тестирования DLP-системы встает вопрос, по каким оценочным критериям должна проводиться оценка соответствия. Оценочные критерии предполагают, чему должна соответствовать DLP-система, и какие процедуры необходимо выполнить для соответствия требованиям приказа ФСТЭК России № 239. Но на данный момент не существует точно определенных критериев для проведения оценки соответствия. Поэтому крайне важно разработать критерии проведения оценки соответствия средств защиты информации, включая DLP-систему.

Некоторые авторы методик проведения оценки соответствия руководствуются в подборе критериев только ИСО/МЭК 15408. Данный стандарт устанавливает требования доверия и требования к функционалу по безопасности. В соответствии с определенным оценочным уровнем доверия выбираются и оценочные критерии. Однако при разработке методик проведения оценки соответствия для ЗОКИИ нецелесообразно опираться только на один документ. В профиле защиты ФСТЭК России описаны требования доверия, которые соответствуют необходимым требованиям безопасности. С учетом стандарта ИСО/МЭК 15408 и профилей защиты, возможно скорректировать требования доверия и требования к функционалу безопасности и, соответственно, подобрать оптимальные оценочные критерии для проведения оценки соответствия DLP-систем и других систем защиты информации. Анализ защищенности автоматизированных систем является одним из ключевых аспектов построения надежной системы обеспечения информационной безопасности предприятия [10].

## *Результаты*

Результатом проведения оценки соответствия является документ (аттестат), подтверждающий, что информационная система соответствует самым актуальным требованиям ФСТЭК России, в том числе:

– предупреждение реализации возможных актуальных угроз безопасности;

– нейтрализацию соответствующих актуальных угроз безопасности информации;

– отсутствие уязвимостей;

– соответствие классу средств защиты информации, установленному для 1 категории ЗОКИИ;

– выявление потенциальных внутренних нарушителей безопасности информации.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/42128 (дата обращения: 15.03.2019).

2. Исследование ИБ-инцидентов, сопряженных с деструктивными действиями увольняющихся сотрудников. Аналитический центр InfoWatch, 2018 [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/report_ueba2017 (дата обращения: 15.03.2019).

3. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: https://minjust.-consultant.ru/documents/38914 (дата обращения: 15.03.2019).

4. Утечки данных. Россия. Аналитический центр InfoWatch, 2018 [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/report_ru2017 (дата обращения: 15.03.2019).

5. Профиль защиты операционных систем типа «А» четвертого класса защиты: Методический документ ФСТЭК России [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/1283 (дата обращения: 15.03.2019).

6. Глобальное исследование утечек конфиденциальной информации в I полугодии 2018 г. Аналитический центр InfoWatch, 2018 [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/report2018_half (дата обращения: 15.03.2019).

7. Исследование утечек конфиденциальной информации из медицинских учреждений в 2017 году. Аналитический центр InfoWatch, 2018 [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/report_med2018 (дата обращения: 15.03.2019).

8. Гатчин Ю. А., Климова Е. В. Основы информационной безопасности : учеб. пособие. – СПб. : ИТМО, 2009. – 85 с.

9. Казарин О. В., Забабурин А. С. Программно-апаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов. – М. : Юрайт, 2019. – 313 с.

10. Петренко С. А., Курбатов В. А. Политики безопасности компании при работе в интернет. – 2-е изд-е. – М. : ДМК, 2012. – 396 с.