УДК 004.054.53
DOI: 10.33764/2618-981X-2019-6-1-115-121

ОЦЕНКА ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Анастасия Сергеевна Голдобина
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант; ООО «Акстел-безопасность», 630110, Россия, г. Новосибирск, ул. Авиастроителей, 39, Б, ведущий аналитик информационной безопасности, тел. (923)220-80-89, e-mail: nastya-gold09@mail.ru

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

Компоненты защиты государственной информационной системы представляют собой единый механизм, способный защищать конфиденциальную информацию. Если один из элементов защиты будет работать неэффективно, это станет проблемой для всей системы защиты информации. Государственным информационным системам необходимо учитывать все доступные способы предотвращения утечки информации, для этого операторы должны проводить оценку эффективности. В настоящей статье предложены возможные пути решения проблемы.

Ключевые слова: оценка эффективности, государственная информационная система, система защиты информации.

EFFICIENCY EVALUATION OF PROTECTION TOOLS OF STATE INFORMATION SYSTEMS

Anastasiya S. Goldobina
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate; «Axtel-security» Ltd., 39, B, Aviastroiteley St., Novosibirsk, 630110, Russia, Lead Information Security Analyst, phone: (923) 220-80-89, e-mail: nastya-gold09@mail.ru

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

Protection components of state information system represent the uniform mechanism capable to protect confidential information. If one of protection elements does not work effectively, it will become a problem for the entire information security system. Public information systems need to take into account all available ways to prevent information leakage, for this, operators should evaluate the efficiency. This article proposes possible solutions of the problem.

Key words: efficiency evaluation, state information system, information protection system.

Введение

Согласно статистике, публикуемой компанией InfoWatch [4], за первое полугодие 2018 г. доля умышленных утечек данных в государственном секторе составляла 42,1 % от общего числа утечек по промышленным отраслям. Самые распространенные каналы утечки информации:

– интернет 69,8 %;
– бумажные документы 10,8 %;
– электронная почта 4,1 % (рисунок).

Гистограмма каналов утечки

Виновниками утечек чаще всего становятся:

– сотрудники 53,5 %;
– руководители 2,3 %;
– бывшие сотрудники 1,9 %;
– системные администраторы 1,2 %.

Доля скомпрометированных данных в государственных органах и силовых структурах за 1-е полугодие 2018 г. достигает 12,9 % от общего числа различных отраслей в Российской Федерации [4].

Статистические данные по утечкам наглядно показывают ситуацию закрытия каналов утечки информации. Государственным информационным системам (далее – ГИС), муниципальным и иным информационным системам для создания системы защиты информации необходимо в максимальной степени учитывать все доступные способы предотвращения утечки информации. В случае отсутствия адекватно настроенной системы защиты информации ущерб может быть причинен не только непосредственно юридическому лицу, но и неопределенно широкому кругу лиц. В ряде случаев за непринятие мер защиты лица,

обладающие ГИС или иными информационными системами, могут быть привлечены к ответственности. Каждый канал утечки информации должен быть проанализирован с точки зрения определения его безопасности и максимально защищен. Создание системы защиты информации от утечек должно осуществляться на профессиональном уровне, с использованием современных технических средств. Для того чтобы система защиты информации позволяла находить и блокировать утечку информации, необходимо внедрить в компании DLP-систему. На российском рынке представлено большое количество DLP-систем с различным функционалом. Огромный выбор данных систем не означает, что все они одинаково действенны для защиты информации от утечек. Чтобы понять, какая из систем лучше удовлетворяет требованиям, необходимо провести оценку эффективности DLP-системы.

В настоящий момент степень изученности алгоритма проведения оценки эффективности DLP-системы крайне мала, некоторые авторы в своих работах предлагали вариант разработки критериев оценки эффективности DLP-системы. Эти критерии полны относительно обычной организации, для которой не требуется проведение оценки эффективности в соответствии с нормативной базой Российской Федерации. Для ГИС необходимо проведение оценки эффективности в рамках аттестационных испытаний системы защиты информации.

Методы и методики

Главной задачей статьи является рассмотрение проблемных вопросов оценки эффективности. Оценка эффективности должна применяться к новой системе защиты информации или уже существующей. С ее помощью система защиты может достичь высоких показателей эффективности, но на практике интеграторы не могут провести качественную оценку эффективности. Она может проводиться как для системы в целом, так и отдельно для внедренных мер и используемых средств защиты информации. В рамках оценки эффективности должны применяться математические методы оценки надежности как системы, так и ее компонентов, методы статистической обработки результатов испытаний и эксплуатации, планирование испытаний, контроля и прогнозирование надежности, а также совершенствование системы защиты информации исходя из полученных результатов.

В настоящий момент оценка эффективности не имеет закрепленных в нормативных документах критериев оценки. Несмотря на это, оценка эффективности включена в состав обязательной аттестации ГИС, которая проводится до ввода в эксплуатацию и вызвана необходимостью официального подтверждения эффективности системы защиты информации в целом или отдельных ее компонентов. В ГИС применяются средства защиты информации, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России, или на соответствие требованиям, указанным в технических условиях (заданиях по безопасности). При этом функции безопасности таких средств должны обеспечивать выполнение этих требований [3].

Аттестат соответствия оператор получает только после разработки программы и методики испытаний. В свою очередь, программа аттестационных испытаний системы должна включать в себя разработку протоколов оценки эффективности принятых мер защиты информации от утечки по техническим каналам. Результаты проведения испытаний системы на соответствие требованиям по защите информации отражаются в оценке эффективности принятых мер при проверке выполнения требований по защите информации от НСД [10].

Без проведения оценки эффективности заявитель не получит аттестат соответствия на систему в целом или на ее компоненты. По результатам аттестационных испытаний оформляется заключение, которое содержит краткую оценку соответствия системы защиты информации объекта информатизации требованиям безопасности информации, рекомендации по контролю за функционированием объекта информатизации.

Оценку соответствия можно представить, как операцию – совокупность действий, мероприятий, направленных на достижение некоторой цели [1] защиты информации, а именно предотвращения ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного или непреднамеренного воздействия на информацию [5].

Тогда оценка эффективности – это выработка оценочного суждения относительно пригодности заданного способа действий или приспособленности технических средств к решению определенных задач на основе измерения уровня эффективности операции [2].

Если воспользоваться приведенным выше определением, используя терминологию [3], то оценка эффективности системы защиты информации – это выработка решения о соответствии системы защиты информации или техники защиты информации установленным требованиям.

На данный момент проведение оценки эффективности системы защиты является неотъемлемой частью процесса создания любой информационной системы, в которой обрабатывается информация ограниченного доступа.

Результаты

В результате проведения оценки эффективности оператор должен получить четкое подтверждение того, что построенная система защиты информации соответствует следующим требованиям:

– она нейтрализует все актуальные угрозы безопасности;

– применяемые средства защиты информации соответствуют предъявляемым требованиям регуляторов.

В настоящее время оценка эффективности ГИС проводится в форме аттестации для официального подтверждения эффективности системы защиты информации, реализованной на объекте информатизации [6]. Из данного документа следует, что аттестация может проводиться в двух формах: добровольная аттестация и обязательная аттестация.

Обязательная аттестация применима к государственным информационным системам. Требования к обязательной аттестации основаны на требованиях регуляторов: федеральные законы, акты Президента Российской Федерации и Правительства Российской Федерации, нормативные правовые акты уполномоченных федеральных органов исполнительной власти. Требования распространяются на определенные виды средств защиты.

Средства управления потоками информации, анализа защищенности, системы мониторинга событий информационной безопасности и другие, не указанные выше, необходимо строить на основе последних профилей защиты, например, сейчас это Профиль защиты операционных систем типа «А» [9].

При этом требования РД НДВ интегрированы в профили защиты. То есть, оператору ГИС в работе по оценке эффективности необходимо совместить достаточно разнородные требования – стандарты 2008 и 2012 гг. сильно различаются.

Стоит учесть, что в подавляющем большинстве случаев субъект может проводить оценку эффективности только инсталлированных (внедренных) средств защиты информации, как минимум, для выявления их влияния на технологический процесс.

С точки зрения Требований оценка эффективности должна пройти на этапах испытаний и приемки системы, необходимые процедуры (компоненты доверия) для стандартов 2008 и 2012 гг. представлены в таблице1 [7, 8].

В ГИС 1-го класса защищенности применяются средства защиты информации (далее – СЗИ) не ниже 4-го класса защиты;

2-й класс защищенности – не ниже 5-го класса защиты;

3-й класс защищенности – не ниже 6-го класса защиты.

Разработка критериев оценивания в соответствии с законодательной базой позволит проверить, насколько DLP-система удовлетворяет заявленным требованиям к системе защиты информации. В то же время, если оценка эффективности является обязательной в рамках проведения аттестации в соответствии с законодательством Российской Федерации, то проведение оценки эффективности DLP-системы является необходимым звеном в цепочке проведения аттестации.

Все указанные процедуры проверки (компоненты доверия) должны быть включены в задание по безопасности, разрабатываемое на основании ГОСТ Р ИСО/МЭК 15446, непосредственно действия по оценке для каждого компонента приведены в ГОСТ Р ИСО/МЭК 18045.

Задания по безопасности для разных версий стандарта 15408 будут разными, их разработка представляет собой нетривиальную задачу и, соответственно, тему отдельного исследования, так же, как и разработка технического отчета об оценке.

Компоненты доверия для 4-го класса защиты

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
Разработка	ADV_ARC.1	Описание архитектуры безопасности
	ADV_FSP.4	Полная функциональная спецификация
	ADV_IMP.2	Полное отображение представления реализации ФБО
	ADV_IMP_EXT.3	Реализация ОО
	ADV_TDS.3	Базовый модульный проект
Руководства	AGD_OPE.1	Руководство пользователя по эксплуатации
	AGD_PRE.1	Подготовительные процедуры
Поддержка жизненного цикла	ALC_CMC.4	Поддержка генерации, процедуры приемки и автоматизация
	ALC_CMS.3	Охват УК представления реализации
	ALC_DEL.1	Процедуры поставки
	ALC_DVS.1	Идентификация мер безопасности
	ALC_FLR.1	Базовое устранение недостатков
	ALC_LCD.1	Определенная разработчиком модель жизненного цикла
	ALC_TAT.1	Полностью определенные инструментальные средства разработки
	ALC_FPU_EXT.1	Процедуры обновления программного обеспечения операционной системы
	ALC_LCD_EXT.3	Определенные разработчиком сроки поддержки
Оценка задания по безопасности	ASE_CCL.1	Утверждения о соответствии
	ASE_ECD.1	Определение расширенных компонентов
	ASE_INT.1	Введение ЗБ
	ASE_OBJ.2	Цели безопасности
	ASE_REQ.2	Производные требования безопасности
	ASE_SPD.1	Определение проблемы безопасности
	ASE_TSS.1	Краткая спецификация ОО
Тестирование	ATE_COV.2	Анализ покрытия
	ATE_DPT.1	Тестирование: базовый проект
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_VAN.5	Усиленный методический анализ
	AVA_CCA_EXT.1	Анализ скрытых каналов
Поддержка доверия	AMA_SIA_EXT.3	Анализ влияния обновлений на безопасность операционной системы

Все указанные документы и процедуры должны быть интегрированы в этапы испытаний ГИС. Помимо вышеописанных процедур рекомендуется прибегать к процедуре испытаний, так как она наиболее близка к рассматри-

ваемым процедурам. Таким образом, процедура испытаний обладает высокой гибкостью, что позволяет на заключительном этапе получить результирующий документ – оценку эффективности.

Заключение

Таким образом, процедура оценки эффективности, проводимая оператором ГИС, является сложной и трудоемкой и требует проведения значительных предварительных исследований. Разработка критериев оценивания в соответствии с законодательной базой позволит проверить, насколько DLP-система удовлетворяет заявленным требованиям к системе защиты информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Надежность и эффективность в технике. Справочник в 10-ти томах. Том 1. Методология. Организация терминология / Издательство Машиностроение. 1986.

2. Надежность и эффективность в технике. Справочник в 10-ти томах. Том 2. Эффективность технических систем / Издательство Машиностроение. 1986.

3. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (ред. от 15.02.2017) [Электронный ресурс]: Приказ ФСТЭК от 11.02.2013 № 17. – Доступ из справ.-правовой системы «Консультант Плюс».

4. Глобальное исследование утечек конфиденциальной информации в I полугодии 2018 г. [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/report2018_half (дата обращения: 12.03.2018).

5. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Введен 1 февраля 2008 г.

6. ГОСТ РО 0043-004-2012. Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний / Для служебного пользования.

7. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200101777, свободный (дата обращения: 10.03.2019).

8. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200101777, свободный (дата обращения: 10.03.2019).

9. Методический документ ФСТЭК России. «Профиль защиты операционных систем типа «А» [Электронный ресурс]. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty/1251-metodicheskie-dokumenty-utverzhdeny-fstek-rossii-8-fevralya-2017-g, свободный (дата обращения: 10.03.2019).

10. ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие положения./ Для служебного пользования.