УДК 004.054.53
DOI: 10.33764/2618-981X-2020-6-1-155-160

ПРОВЕДЕНИЕ ОЦЕНКИ СООТВЕТСТВИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ЗНАЧИМЫХ ОБЪЕКТАХ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Анастасия Сергеевна Голдобина
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры информационной безопасности, тел. (923) 220-80-89, e-mail: nastya-gold09@mail.ru

Дмитрий Михайлович Никулин
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент кафедры фотоники и приборостроения, тел. (383) 343-91-11, e-mail: dimflint@mail.ru

Необходимость проведения оценки соответствия средств защиты информации обусловлена важностью самой информации, обрабатываемой на предприятии. Отсутствие конкретных требований и критериев для проведения оценки станет причиной некорректного функционирования средств защиты, что в свою очередь приведет к непредсказуемым последствиям, а также к нарушению функционирования значимых объектов. Даже с учетом внесенных в законодательство РФ изменений нет определенного алгоритма проведения оценки соответствия средств защиты определенных классов, таких как DLP-системы. В настоящей статье описаны внесенные в законодательство изменения и как они повлияют на процесс проведения оценки соответствия. Выбранный профиль защиты, наравне с ГОСТом 15408-2012, раскрывают такие понятия как функциональные требования доверия и функции безопасности. С учетом этих нормативных правовых актов можно разработать метод проведения оценки соответствия для DLP-систем, которые являются крайне важным средством защиты от утечек конфиденциальной информации на значимых объектах критических информационных инфраструктур.

Ключевые слова: оценка соответствия, значимый объект, критическая информационная инфраструктура, безопасность информации, защита информации, DLP-системы.

ASSESSMENT OF COMPLIANCE OF INFORMATION SECURITY MEANS ON SIGNIFICANT OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURES OF THE RUSSIAN FEDERATION

Julia A. Isaeva
Siberian state University of geosystems and technologies, 10, Plahotnogo St., Novosibirsk, 630108, Russia, Graduate, Institute of Optics and Information Security Technologies, phone: (913) 980-23-09, e-mail: Isaeva.JA@hotmail.com

Anastasiya S. Goldobina
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Institute of Optics and Information Security Technologies; phone: (923) 220-80-89, e-mail: nastya-gold09@mail.ru

Dmitry M. Nikulin
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Head of the Department of Photonics and Instrumentation, phone: (383) 343-91-11, e-mail: dimflint@mail.ru

The need to assess the compliance of information security means depends on the importance of the information, processed at the enterprise. The lack of specific requirements and criteria for conducting an assessment will cause the protection tools to function incorrectly this, in turn, will lead to unpredictable consequences, as well as to the disruption of the functioning of significant objects. Even with the changes made to the legislation of the Russian Federation, there is no specific algorithm for assessment the compliance of certain classes of security tools, such as DLP systems. This article describes the changes made to the legislation and how they will affect the compliance assessment process. The selected security profile, along with GOST 15408-2012, reveals such concepts as functional requirements of trust and security functions. Taking these regulations into account, it is possible to develop a method for conducting compliance assessment for DLP systems, which are an extremely important means of protecting against leaks of confidential information on significant objects of critical information infrastructures.

Key words: compliance assessment, significant object, critical information infrastructure, information security, information protection, DLP systems.

Введение

Развитие информационных технологий предполагает также и развитие нормативных правовых актов, федеральных законов и постановлений правительства.

В связи с появлением федерального закона № 187 [1], а также приказа ФСТЭК России № 239 [2], возник новый сегмент информационных систем, в который входят большое количество различных объектов. Группа этих объектов делится на информационно-телекоммуникационные сети, автоматизированные системы управления технологическим процессом и информационные системы.

В указанных выше документах описаны пункты по обеспечению требований безопасности. Такие требования должны содержать конкретные указания на состав организационных и технических мер, необходимых для обеспечения безопасности информации, содержащейся в информационных системах предприятий. Помимо организационных и технических мер, в законодательстве должны быть описаны правила настройки средств защиты информации для обеспечения необходимого уровня безопасности информации. Однако конкретные критерии в данных требованиях отсутствуют.

Методы и материалы

В 2019 году были внесены поправки в приказы ФСТЭК России 239 и 17, что ознаменовало переход к новой системе требований предъявляемых к средствам защиты информации.

Теперь система требований к оценке основывается на уровнях доверия, устанавливаемых приказом [3]. Дополнительно к данному приказу вышла мето-

дика выявления уязвимостей и недекларированных возможностей в программном обеспечении.

Таким образом, требования по безопасности в общем виде сейчас состоят из двух разделов:

– функциональных требований к безопасности, установленных соответствующими профилями защиты;

– уровнями доверия, установленными приказом ФСТЭК России № 131, фактически заменившим в профиле защиты оценочный уровень доверия.

Рассматривая вопросы оценки средств защиты, применяемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры (далее – ЗО КИИ), перед исследователем встает вопрос, насколько требования стали жестче или мягче, и насколько выросли затраты.

Приказ [3] включает в себя только требования и не предоставляет пользователям ни методологии оценки эффективности, ни требований к разработке, оформлению и содержанию документов.

Таким образом, перед владельцем значимого объекта критической информационной инфраструктуры в 2020 году стоит нетривиальная задача проведения оценки соответствия по совершенно новым процедурам.

Различные средства защиты информации предполагают также и различную настройку функционала, задание определенных правил, подпадающих под возможности выбранного средства. В данном случае будем рассматривать такой класс средств защиты информации как Data Loss Prevention (далее DLP-система). Это программный продукт, созданный для предотвращения утечек конфиденциальной информации за пределы корпоративной сети. Эта система строится на анализе потоков данных, выходящих за пределы корпоративной сети.

Выбор такого класса средств защиты информации обусловлен количеством утечек конфиденциальной информации. По данным статистического анализа компании InfoWatch в первом полугодии 2019 года в мире обнародовано и зарегистрировано аналитическим центром InfoWatch 1276 случаев утечки конфиденциальной информации [10]. Это на 22% превышает количество инцидентов, зарегистрированных за аналогичный период 2018 года. Для более наглядного примера количество скомпрометированных записей персональных данных по сравнению с аналогичным периодом 2018 года выросло в 3,6 раза и составило 8,74 млрд [10].

Результаты

Учитывая приведенную статистику, можно отметить, что класс средств защиты как DLP-системы сейчас достаточно востребован. При внедрении и использовании данной системы на предприятии становится возможным предотвращение утечек конфиденциальной информации, а, значит, в результате существенное снижение процентного соотношения утечек конфиденциальной информации по мировому уровню.

Однако данный класс средств защиты представляет собой достаточной сложную систему в процессе настройки. Возникает необходимость внедрить систему на предприятие с уже существующей информационной системой, а значит – необходимо подстроиться под определенную подсистему безопасности. При этом нужно сохранить максимальную работоспособность всей информационной системы и подсистемы безопасности в частности.

Для настройки средств защиты информации должна существовать методика или правила, чтобы обеспечить корректное функционирование системы безопасности. Необходимо, чтобы такие правила соответствовали определенным требованиям, указанным в законодательстве РФ. В таком случае используются выше указанные приказы ФСТЭК России № 239, 131 и федеральный закон № 187. И соответственно, после установки и настройки средства защиты информации необходимо, чтобы DLP-система прошла оценку соответствия.

При использовании «Общих критериев» объект оценки (далее - ОО), которым в данном случае будет являться DLP-система, рассматривается в контексте окружающей его среды функционирования. Следовательно, перед внедрение DLP-системы, необходимо изучить информационную систему, уже имеющуюся на предприятии. Крайне важно учитывать составляющие этой системы, так как может возникнуть ситуация, при которой внедрение определенной DLP-системы невозможно.

Таким образом, для обеспечения безопасности необходимо, чтобы предприятия, относящиеся к ЗО КИИ, имели единый регламент для установки и настройки средств защиты безопасности. При этом сохраняется возможность адаптированной настройки средств защиты, подходящей для определенных подсистем безопасности. Такая возможность является очень важной при внедрении программного обеспечения как в новую информационную систему, так и в уже существующую. Важность такой возможности обусловлена изменяемостью информационных систем на современных предприятиях.

В таблице представлены функциональные требования безопасности, предъявляемые к DLP-системам.

Функциональные требования безопасности

Функциональные требования безопасности, предъявляемые к DLP-системам Условное обозначение семейства	Наименование функциональной возможности
FMT_MTD	Управление данными функций безопасности DLP-системы
FMT_SMR	Назначение административных ролей управления безопасностью
FAU_GEN	Генерация данных аудита безопасности
FAU_SAR	Просмотр аудита безопасности
FDP_DAU	Аутентификация данных пользователя
FIA_UID	Выбор момента идентификации пользователя

Функциональные требования должны перекрываться функциями DLP-систем, а также функциями операционной системы, в которой будет установлена DLP-система. Так как такая операционная система по типу будет являться серверной, то для выполнения требований безопасности также необходимо использовать доменные службы Active Directory.

Заключение

DLP-системы могут работать совместно с доменными службами, что облегчает настройку и аудит данных.

Также стоит отметить, что необходимо распределить по этапам создания подсистемы обеспечения безопасности ЗО КИИ, при этом необходимо учесть, что DLP-система является лишь одной из составных частей системы обеспечения безопасности, при этом ее работа сильно зависит от остальных компонентов.

Исходя из приведенного выше, а также опираясь на положения ГОСТ РО 0043-3-2014, следует отметить, что наиболее оптимальной процедурой для проведения оценки соответствия с учетом стандартов ИСО/МЭК 15408 в рамках Приказа ФСТЭК России № 239 является аттестация по требованиям безопасности информации, в рамках которой осуществляется подтверждение соответствия средств защиты информации требованиям, представленным в пункте 29 приказа ФСТЭК России [2]. Аттестационные испытания не является обязательными для большей части ЗО КИИ, однако при их применении возможно повысить достоверность полученных результатов.

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, свободный (дата обращения: 10.03.2019).

2. 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/docu-ments/38914, свободный (дата обращения: 10.03.2019).

3. Приказ ФСТЭК России от 28 февраля 2017 г. № 31 ДСП «Требования к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых организациями оборонно-промышленного комплекса».

4. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка)» - Утверждены Приказом ФСТЭК России от 30 июля 2018 г. № 131.

5. 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).

6. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200105710, свободный (дата обращения: 10.03.2019).

7. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200105711, свободный (дата обращения: 10.03.2019).

8. ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200105309, свободный (дата обращения: 10.03.2019).

9. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / Под.ред. А.С. Маркова. М., Радио и связь, 2012. 192 с.

10. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года / Аналитический центр InfoWatch. 2019. 30 с.