УДК 004.054.53
DOI: 10.33764/2618-981X-2019-9-25-29

АНАЛИЗ РАЗВИТИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Валентин Валерьевич Селифанов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: sfo1@mail.ru

Оксана Владимировна Ермак
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, студент, тел. (923)174-90-59, e-mail: oksana.ermak@inbox.ru

Анна Владимировна Якунина
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, студент, тел. (913)707-36-48, e-mail: aniyaaa99@mail.ru

Карина Викторовна Яркова
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, студент, тел. (961)219-75-46, e-mail: 61ka16@gmail.com

Процесс развития средств защиты информации можно разделить на три этапа: изобретение письменности, появление технических средств обработки информации и период массовой информатизации общества. Каждый этап характеризуется развитием носителей информации, в результате которого появляются новые угрозы утечки информации. В связи с этим возникает необходимость формирования требований к средствам защиты информации, информационных систем.

Ключевые слова:средство защиты информации, информация, требования, методы защиты информации, система, средство обработки информации, угроза утечки информации.

ANALYSIS OF THE DEVELOPMENT OF MEANS OF INFORMATION PROTECTION

Valentin V. Selifanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (383)343-91-11, e-mail: sfo1@mail.ru

Oksana V. Ermak
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk 630099, Russia, Student, phone: (923)174-90-59, e-mail: oksana.ermak@inbox.ru

Anna V. Yakunina
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk 630099, Russia, Student, phone: (913)707-36-48, e-mail: aniyaaa99@mail.ru

Karina V. Yarkova
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk 630099, Russia, Student, phone: (961)219-75-46, e-mail: 61ka16@gmail.com

The process of the development of means of information protection can be divided into three stages: invention of writing, emergence of technical means of information processing and period of mass Informatization of society. Each stage is characterized by the development of information carriers, as a result of which there are new threats of information leakage. In this connection there is a necessity of formation of requirements to protection of information and information systems.

Key words: means of information protection, information, requirements, methods of information protection, system, means of information processing, threat of information leakage.

Средство защиты информации – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации [1], которое может обеспечивать защиту всех составных частей.

Процесс формирования методов и средств защиты информации можно поделить на три периода. Деление происходит на основе эволюции видов носителей информации.

С каждым годом финансовые потери, приносимые вирусными атаками на компьютерные сети становятся все больше. Наиболее известным примером является вирус «Iloveyou», так как данная «эпидемия» вывела из строя более 5 миллионов компьютеров и нанесла ущерб свыше 10 миллиардов долларов. Вирус распространялся через электронную почту пользователей MicrosoftOutlook и уничтожал или изменял некоторые файлы на зараженном компьютере. Кроме того, червь сразу же, в момент запуска, рассылал себя по всем адресам адресной книги пользователя [2].

Интересным фактом в сфере информационной безопасности является вывод о том, что утечка хотя бы 20 % информации, касающейся данных о коммерческой организации, в шестидесяти случаях из ста приводит к ее банкротству.

Гостехкомиссия России (сейчас Федеральная служба по техническому и экспортному контролю – ФСТЭК России) в период с 1992 по 1999 г. разработала пакет руководящих документов, посвященных вопросам защиты информации в автоматизированных системах. Также был разработан ГОСТ Р ИСО/МЭК 15408-2-2002, в котором описываются требования безопасности информационных технологий объекта оценки, излагаемых в профиле защиты или в задании по безопасности, на данный момент действует ГОСТ Р ИСО/МЭК 15408-2-2013 [3].

Для того, чтобы не происходила утечка данных, необходимо разрабатывать и своевременно обновлять требования к средствам защиты информации. Сейчас происходит постепенный переход к «требованиям нового поколения», которые пока представлены, следующим набором документов.

Приказ ФСТЭК России от 3 апреля 2018 г. №55. Положение о системе сертификации средств защиты информации [4], устанавливаливающее основные принципы, организационную структуру системы обязательной сертификации средств защиты информации, порядок проведения сертификации этих средств по требованиям безопасности информации, а также государственного контроля и надзора за сертификацией и сертифицированными средствами защиты информации.

Приказ ФСТЭК России от 15 марта 2012 г. №638. Требования к системам обнаружения вторжения [5]. Данные требования применяются к программным и программно-техническим средствам, которые используются для обеспечения защиты информации, составляющих сведения с ограниченным доступом.

Приказ ФСТЭК России от 1 августа 2012 г. №28. Требования к средствам антивирусной защиты [6]. Данные требования применяются к программным средствам, используемым в целях обеспечения защиты информации, которые содержат сведения ограниченного доступа.

Приказ ФСТЭК России от 1 января 2014 г. №119. Требования к средствам доверенной загрузки [7]. Данные требования к средствам доверенной загрузки применяются к программным и программно-техническим средствам, используемым для обеспечения защиты информации, которые содержат сведения ограниченного доступа и предотвращают несанкционированный доступ к программным и (или) техническим ресурсам.

Приказ ФСТЭК России от 1 декабря 2014 г. №87. Требования к средствам контроля съемных машинных носителей информации [8]. Данные требования применяются к программным и программно-техническим средствам, которые используются в целях обеспечения защиты информации, которые содержат информацию ограниченного доступа и предотвращают несанкционированный доступ к программным и (или) техническим ресурсам.

Приказ ФСТЭК России от 1 декабря 2016 г. №9. Требования к межсетевым экранам [9]. Данные требования применяются к программным и программно-техническим средствам, которые реализуют функции контроля и фильтрации и используются в целях обеспечения защиты информации, содержащей сведения ограниченного доступа.

Приказ ФСТЭК России от 1 июня 2017 г. №119. Требования безопасности информации к операционным системам [10]. Данные требования применяются к операционным системам, которые используются для обеспечения защиты информации, содержащей сведения ограниченного доступа при ее обработке в информационных системах.

Как видно, средствам обеспечения безопасного межсетевого взаимодействия, сейчас уделяется достаточно большое внимание. Эти средства должны учитывать все применяемые информационные технологии.

Вслед за бурным развитием информационных технологий появляются все новые и новые угрозы. Для того, чтобы им противостоять активно внедряются такие средства защиты как DLP и SIEM.

DLP-система (Data Loss Prevention) – это программный продукт, созданный для предотвращения утечек конфиденциальной информации за пределы корпоративной сети.

Наиболее часто DLP-системы применяются для решения следующих неосновных для себя задач:

— мониторинг общения сотрудников с целью выявления «подковерной» борьбы, которая может навредить организации;

— контроль использования рабочего времени и рабочих ресурсов сотрудниками;

— выявление сотрудников, рассылающих резюме, для оперативного поиска специалистов на освободившуюся должность;

— контроль правомерности действий сотрудников (предотвращение печати поддельных документов и пр.).

SIEM-системы появились в результате эволюции и слияния SEM и SIM.

SEM (Security Event Management) – система защиты, работающая в режиме реального времени. Она самопроизвольно отслеживает события в информационных потоках и собирает их.

SIM (Security Information Management) – система, отвечающая за анализ сведений на основе статистики и отклонений от установленных правил безопасности.

SIEM-решение позволяет обнаружить: внешние и внутренние атаки; отдельные заражения вирусами; попытки получить несанкционированный доступ к защищаемой информации; нарушения в работе информационных систем; слабые точки защиты; нарушения структуры средств защиты.

SIEM-система может: анализировать события и предупреждать при возникновении каких-либо отклонений; проверять на соответствие стандартам; создавать отчеты, в том числе настроенные пользователями; мониторить события от устройств или серверов и создавать соответствующие оповещения для заинтересованных лиц; избавлять от рисков при наличии сканера уязвимостей.

В то же время такие системы, как DLP и SIEM, не имеют четко установленных требований по информационной безопасности.

В связи с повлением новых тенденций в развитии информационных технологий становятся востребованными новые функции DLP-систем. Глобальное использование мобильных устройств при ведении бизнеса послужило причиной возникновения мобильного DLP. Создание корпоративных и публичных «облаков» потребовало защиты, в том числе и DLP-системами. Все это привело к появлению «облачных» сервисов инфоормационной безопасности.

Одной из компаний лидеров производителей DLP-систем из зарубежных компаний является Symantec Corp., на российском рынке популярны продукты отечественных разработчиков DLP-систем: Info Watch End Point Security, Sola rDozor.

На данном этапе многие крупные компании и государственные учреждения являются главными потребителями SIEM-систем. Так как они отвечают таким качествам, как: производительность, масштабируемость, отказоустойчивость также немаловажным фактором является соотношение «цена-качество». Государственные учреждения большое внимание уделяют на наличие сертификатов соответствия требованиям регуляторов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р50922-2006 «Защита информации. Основные термины и определения» [Электронный документ] URL: http://www.altell.ru/legislation/standards/50922-2006.pdf.

2. Начало эпидемии ILOVEYOU [Электронный документ] URL: https://www.securitylab.ru/informer/240711.php.

3. ГОСТ Р ИСО/МЭК 15408-2-2013«Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий» [Электронный документ] URL: http://www.internet-law.ru/gosts/gost/6112/

4. Об утверждении Положения о системе сертификации средств защиты инфорации: приказ ФСТЭК России от 03.04.2018 №55 / [Электронный ресурс] / Режим доступа: www.consultant.ru

5. Об утверждении требований к системам обнаружения вторжений: информационное письмо ФСТЭК России от 01.03.2012 №240 / [Электронный ресурс] / Режим доступа: www.consultant.ru

6. Об утверждении требований к средствам антивирусной защиты: информационное сообщение ФСТЭК России от 30.07.2012 №240/24/3095 / [Электронный ресурс] / Режим доступа: www.consultant.ru

7. Об утверждении требований к средствам доверенной загрузки: информационное письмо ФСТЭК России от 06.02.2014 №240/24/405 / [Электронный ресурс] / Режим доступа: www.consultant.ru

8. Об утверждении требований к средствам контроля съемных машинных носителей информации: информационное сообщение ФСТЭК России от 24.12.2014 №240/24/4918 / [Электронный ресурс] / Режим доступа: www.consultant.ru

9. Об утверждении требований к межсетевым экранам: информационное сообщение ФСТЭК России от 28.04.2016 № 240/24/1986 / [Электронный ресурс] / Режим доступа: www.fstec.ru

10. Об утверждении требований безопасности информации к операционным системам: информационное сообщение ФСТЭК России от 18.10.2016 № 240/24/4893 / [Электронный ресурс] /Режим доступа: fstec.ru