УДК 004.056.5

А.С. Шабуров, В.И. Борисов

Пермский национальный исследовательский политехнический университет,
Пермь, Россия

РАЗРАБОТКА МОДЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ КОРПОРАТИВНОЙ СЕТИ НА ОСНОВЕ ВНЕДРЕНИЯ SIEM-СИСТЕМЫ

Сформулирована актуальная проблема обнаружения и локализации вредоносной информации, находящейся внутри корпоративных сетей, в больших информационных массивах. Определены основные исходные данные для формирования необходимого перечня способов и средств защиты информации. Обусловлена необходимость применения разнообразных автоматизированных средств и систем для решения задач обеспечения информационной безопасности. Приведена характеристика SIEM-систем как одного из современных подходов в решении задач защиты информации корпоративных сетей. Перечислены основные задачи, решаемые на основе внедрения и эксплуатации SIEM-системы, а также типовые функциональные возможности при выявлении событий и инцидентов информационной безопасности. Приведены типовая структура при внедрении основных компонентов SIEM-системы и детализация функциональных уровней работы системы. Сформулированы условия для построения эффективной системы защиты информации на основе внедрения SIEM-системы. Разработана структурно-функциональная модель SIEM-системы. Определен и рассчитан состав основных аппаратных ресурсов информационной системы, достаточных для обеспечения эффективной работы SIEM-системы. Приведено описание настроек системы и процедуры написания правил как последовательность необходимых действий. Разработана схема алгоритма написания правил. Перечислены стадии написания правил. Рассмотрена стадия написания правила на примере обнаружения TCP, ICMP, UDP подключений из подгрупп, не имеющих права выхода в Интернет. Для этого проведена проверка работоспособности регулярного выражения. Создано правило в редакторе QRadar, и для него выбраны необходимые правила срабатывания SIEM-системы. Проведены настройки правил посредством настройки свойств инцидента, генерируемого при срабатывании правила. Сделаны необходимые выводы.

Ключевые слова: объект информатизации, защита информации, SIEM-система, лог-файлы, структурно-функциональная модель, событие информационной безопасности, имитация инцидента.

A.S. Shaburov, V.I. Borisov

Perm National Research Polytechnic University, Perm, Russian Federation

DEVELOPING MODEL INFORMATION PROTECTION CORPORATE NETWORK BASED ON THE IMPLEMENTATION OF SIEM-SYSTEM

The actual problem of detection and localization of the malicious information which is in corporate networks in big information massifs is formulated. Basic data for formation of the necessary list of ways and means of information protection are defined. The characteristic of SIEM systems as one of modern approaches in the solution of tasks of information security of corporate networks is provided. The main objectives solved on the basis of introduction and operation of SIEM system and also standard functionality at identification of events and incidents of information security are listed. The typical structure at introduction of the main components of SIEM system is given and specification of functional levels of work of system. Conditions for creation of effective system of information security on the basis of implementation of SIEM system are formulated. The structurally functional model of SIEM system is developed. The structure of the main hardware resources of information system sufficient for ensuring effective work of SIEM system is determined and calculated. The description of settings of system, and procedure of writing of rules as sequence of necessary actions is provided. The scheme of algorithm writing of rules is developed. Stages of writing of the rule are listed. The stage of writing the rule on the example of detection of TCP, ICMP, UDP connections from the subgroups which don't have the right of Internet connection is considered. An inspection of operability of regular expression is for this purpose carried out. It is created rules in the QRadar editor and for this rule and necessary rules of operation of SIEM system are chosen. Setting up rules by means of control properties of the incident generated at operation of the rule is carried out. Necessary conclusions are drawn.

Keywords: object of informatization, information security, SIEM system, log files, structurally functional model, event of information security, incident imitation.

Развитие и разнообразие бизнес-процессов обуславливают увеличение интенсивности информационного обмена в информационных системах. В настоящее время актуальной проблемой является проблема обнаружения и локализации вредоносной информации, находящейся внутри корпоративных сетей. Также растут количество и разнообразие информационных атак на ресурсы информационных систем.

Способы проникновения вредоносной информации в корпоративные информационные системы также стремительно модифицируются, что делает процесс нахождения вредоносной информации более трудоемким и требующим применения различных средств защиты информации.

Интенсивность информационных событий в корпоративных сетях может достигать нескольких миллионов в день, поэтому возникает проблема нахождения и локализации вредоносной информации в огромных информационных массивах. При этом обработка подобных

событий в ручном режиме не представляется возможной, так как потребовала бы значительных человеческих и временных затрат, а также недопустимых с точки зрения эффективности аппаратно-программных ресурсов [1].

Для построения эффективной, в том числе и с экономической точки зрения, системы защиты информации необходимо определить и проанализировать основные проблемы защиты информации на объектах информатизации конкретной компании.

Под объектом информатизации понимается совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией. Помимо перечисленного защиты требуют средства обеспечения объектов, помещений, в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [2].

В ходе анализа проблемы защиты информации на объектах информатизации, на основании особенностей каждого объекта, необходимо определить информационные ресурсы, которые используются в данной информационной системе. К ним, как правило, относятся:

- файловые сервисы;
- локальные вычислительные сети;
- серверы баз данных;
- серверы приложений;
- офисные приложения;
- системы виртуализации.

Также необходимо определить категории доступности информации, обрабатываемой в данной информационной системе. После этого составляется перечень основных технических средств и систем, с помощью которых происходит обработка информации ограниченного доступа.

Анализ проблем безопасности информации предполагает определение основных факторов, влияющих на организацию комплексной системы защиты информации. Прежде всего к ним относятся форма собственности предприятия, сфера основных видов деятельности, особенности территориального расположения предприятия, степень автоматизации основных процедур обработки защищаемой информации и ряд других факторов [3].

На основании существенных факторов, объекта защиты информации, анализа и оценки угроз, как правило, формируется необходимый перечень способов и средств защиты информации. При этом интенсивность информационного обмена, сложность современных алгоритмов обработки информации, разнообразие угроз и средств защиты от них обусловливают необходимость применения разнообразных автоматизированных средств и систем для решения задач обеспечения информационной безопасности.

Одним из современных подходов к решению задач защиты информации корпоративных сетей является внедрение внедрения SIEM-технологии.

SIEM (Security information event management) – класс систем обеспечения информационной безопасности, появившихся в результате слияния SEM-систем и SIM-систем. Основным функциональным отличием данных систем является то, что SEM-системы предназначены для анализа информации в режиме реального времени, а SIM-системы анализируют уже накопленную информацию [4].

Основной функцией SIEM-систем является анализ информации, поступающей от разных источников, таких как системы DLP, средства антивирусной защиты информации, межсетевые экраны, системы учета трафика, сканеры уязвимости и т.д. [5]. На основе анализа данных из этих источников выявляются отклонения от нормального функционирования, заданного критериями безопасности, и в случае обнаружения происходит оповещение администратора безопасности.

Кроме того, типовая SIEM-система может использоваться для [6]:

– анализа информации, поступающей от различных источников;

– предоставления доказательной базы при расследовании инцидентов информационной безопасности;

– предоставления структурированной информации, необходимой при аудите информационной безопасности;

– обеспечения непрерывности работы сервисов путем обнаружения сбоев в их работе;

– структуризации информационно-телекоммуникационной системы.

Типовые функциональные возможности SIEM-систем предполагают выявление следующих событий и инцидентов информационной безопасности:

– сетевых атак во внутреннем и внешнем периметрах;

– вирусных эпидемий или отдельных вирусных заражений;

– попыток несанкционированного доступа к конфиденциальной информации;

– мошенничества;

– ошибок и сбоев в работе информационных систем;

– уязвимостей различной природы;

– ошибок конфигураций в средствах защиты и информационных системах;

– целевых атак.

Основными задачами обеспечения информационной безопасности, которые ставятся перед SIEM-системой, как правило, являются следующие:

– централизованное хранение журналов событий;

– обработка и корреляция событий;

– оповещение об инцидентах;

– расследование инцидентов;

– управление инцидентами (инцидент-менеджмент).

Типовое решение SIEM-системы включает в себя несколько функциональных компонентов (рис. 1):

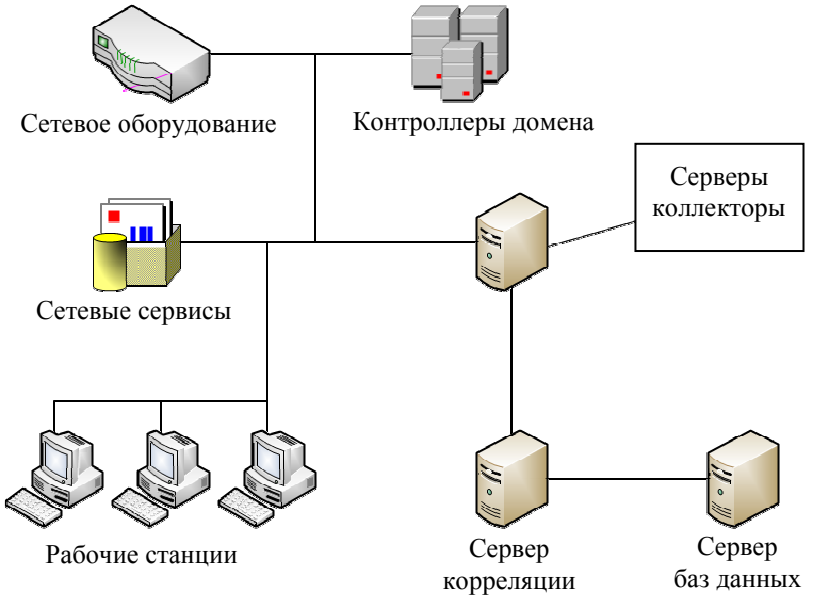

Рис. 1. Структура основных компонентов SIEM-систем

– агенты, устанавливаемые на инспектируемую информационную систему (актуально для операционных систем; агент представляет собой резидентную программу (сервис, демон, служба), которая локально собирает журналы событий и по возможности передает их на сервер);

– коллекторы на агентах, которые, по сути, представляют собой модули (библиотеки) для понимания конкретного журнала событий или системы;

– серверы-коллекторы, предназначенные для предварительной аккумуляции событий от множества источников;

– сервер-коррелятор, отвечающий за сбор информации от коллекторов и агентов и обработку по правилам и алгоритмам корреляции;

– сервер баз данных и хранилища, отвечающий за хранение журналов событий.

Функционирование SIEM-системы целесообразно детализировать на несколько уровней [7]:

– сбор лог-файлов и формирование необходимых данных от различных источников;

– нормализация данных, заключающаяся в приведении событий с одинаковым смыслом к общему формату;

– корреляция событий системы, важных для обеспечения безопасности, путем нахождения связей между ними, например, подбор паролей, заражение вредоносным кодом, аномальная активность в системе, изменение критических параметров системы и т.п.;

– организация хранения лог-файлов;

– реагирование на инциденты, в том числе уведомления о важных событиях для информационной безопасности;

– визуализация инцидентов, формирование отчетных документов.

Данная структура является общей для всех информационных систем. При этом для построения эффективной системы защиты информации необходимо учитывать особенности конкретной корпоративной сети. Внедрение любого SIEM-решения с учетом особенностей информационной системы предполагает разработку адекватной структурно-функциональной модели данной системы.

Структурно-функциональная модель системы защиты информации (СЗИ) включает в себя перечень структурных компонентов оборудования, а также их функциональные связи и возможности при решении задачи анализа и защиты информации (рис. 2).

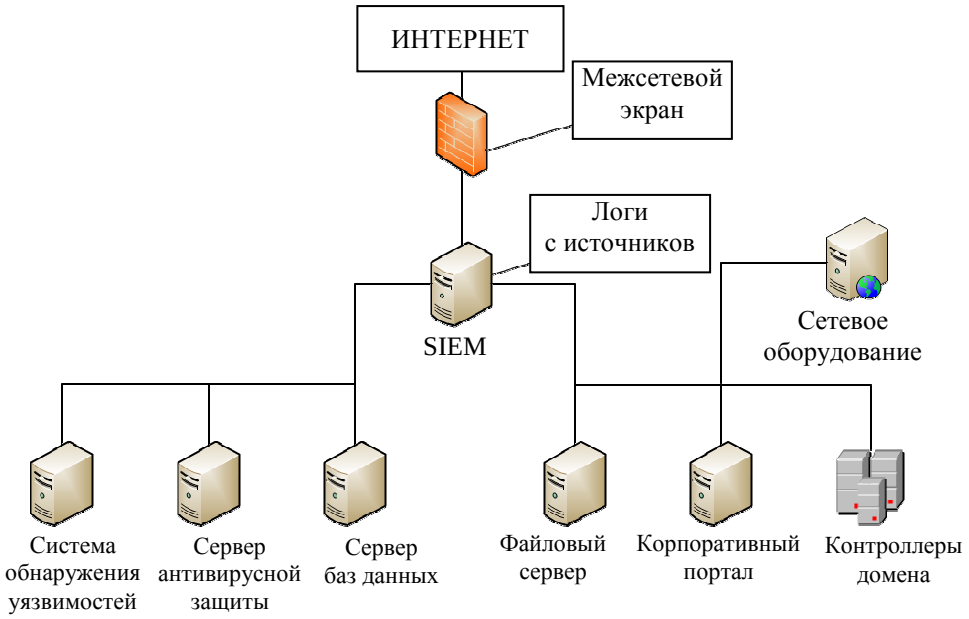

Рис. 2. Структурно-функциональная модель SIEM-системы

К типовым структурным компонентам относятся:

– межсетевой экран;
– почтовые сервисы;
– базы данных;
– система обнаружения уязвимостей;
– антивирусная защита;
– корпоративный портал;
– файловый сервер.

По функциональным возможностям структурные компоненты делятся на несколько групп:

– средства, сканирующие сеть в поисках уязвимостей;
– иные средства;
– межсетевой экран, ограничивающий перемещение пакетов за пределы локальной сети;
– устройства, отправляющие технологии в SIEM-системе.

Построение структурно-функциональной модели с учетом особенностей определенной корпоративной сети позволяет оптимизировать функциональные возможности SIEM-системы и, как следствие, построить более эффективную систему защиты информации.

Функциональные возможности SIEM-системы обеспечиваются определением необходимых и достаточных для достижения целей ее работы аппаратных ресурсов. Аппаратные ресурсы, необходимые для обеспечения стабильной работы SIEM-системы, можно разделить на две основные группы:

– ресурсы для аппаратной части;
– ресурсы для хранения логов.

Ресурсами для аппаратной части являются:

– серверная станция;
– устройство ОЗУ;
– процессоры;
– жесткий диск для работы операционной системы.

Должной уровень отказоустойчивости системы обеспечивается применением RAID/SSD-технологий для хранения информации на жестких дисках.

Для данной системы достаточными будут следующие ресурсы:

– два 12-ядерных процессора с частотой 2,6 GHz;
– 64 Гбайта оперативной памяти;
– 150 Гбайт памяти для системы.

Расчет необходимого объема хранилища логов определяется по формуле [8]

$$F_i = NV_i, \quad (1)$$

где F_i – объем поступающих событий с секунду; N – максимальное число событий в секунду; V_i – средний размер одного события, помещенного в систему хранения.

Кроме того, необходимо учесть дополнительный объем памяти для стабильного быстродействия и зарезервировать дополнительно 20 % места дискового пространства.

Время хранения всех логов, как правило, составляет 90 дней, что сопоставимо с периодом времени, необходимого для составления квартального отчета по работе системы. При этом время хранения инцидентов может зависеть от степени их критичности.

Следовательно, формула нахождения объема хранилища, необходимого для хранения логов, будет иметь вид:

$$F = 1{,}2\sum_{i=1}^{T} F_i , \quad (2)$$

где F – необходимое пространство для хранения логов; F_i – объем поступающих событий в секунду; T – период хранения логов.

Максимальное количество событий в секунду – 1000.

Средний размер одного события – 0,3 Кбайт.

Рассчитанный объем необходимого пространства для хранения логов вычисляется по формуле

$$1{,}2 \cdot \sum_{1}^{7776000} (1000 \cdot 3{,}31 \cdot 10^{-10}) = 3{,}0 \text{ Тб.}$$

После установки SIEM-системы необходимо подключить источники событий информационной безопасности и написать правила обработки данных событий.

Написание правила представляет собой последовательность следующих действий:

– имитация инцидента;

– нахождение записи об этом событии в логах источника;

– определение уникальных атрибутов в коде данного события;

– при необходимости выделение из кода каких либо атрибутов в поле события, используя регулярные выражения (создание парсеров);

– создание правила в редакторе правил QRadar с учетом уникальных атрибутов события;

– повторная имитация инцидента для проверки работоспособности правила.

Схема алгоритма написания правила представлена на рис. 3.

Стадии написания правила целесообразно рассмотреть на примере обнаружения TCP, ICMP, UDP-подключений из подгрупп, не имеющих право выхода в Интернет.

Данное правило срабатывает при обнаружении отправки TCP, ICMP, UDP-пакетов через межсетевой экран. Внутренний нарушитель может перенастроить компьютер и получить доступ в Интернет. В свою очередь, внешний нарушитель потенциально может получить доступ к компьютеру через Интернет и, как следствие, доступ в корпоративную сеть. Для имитации инцидента с компьютера, не имеющего выхода в Интернет, был отправлен запрос на ресурс с IP-адресом 1.2.3.4. Далее была найдена запись данного события. Было обнаружено, что QRadar определил не все информационные поля, в частности название протокола. Поскольку это поле является важным для данного правила, в дальнейшем разработано правило выделения свойства. Для этого использовались так называемые «регулярные выражения» системы.

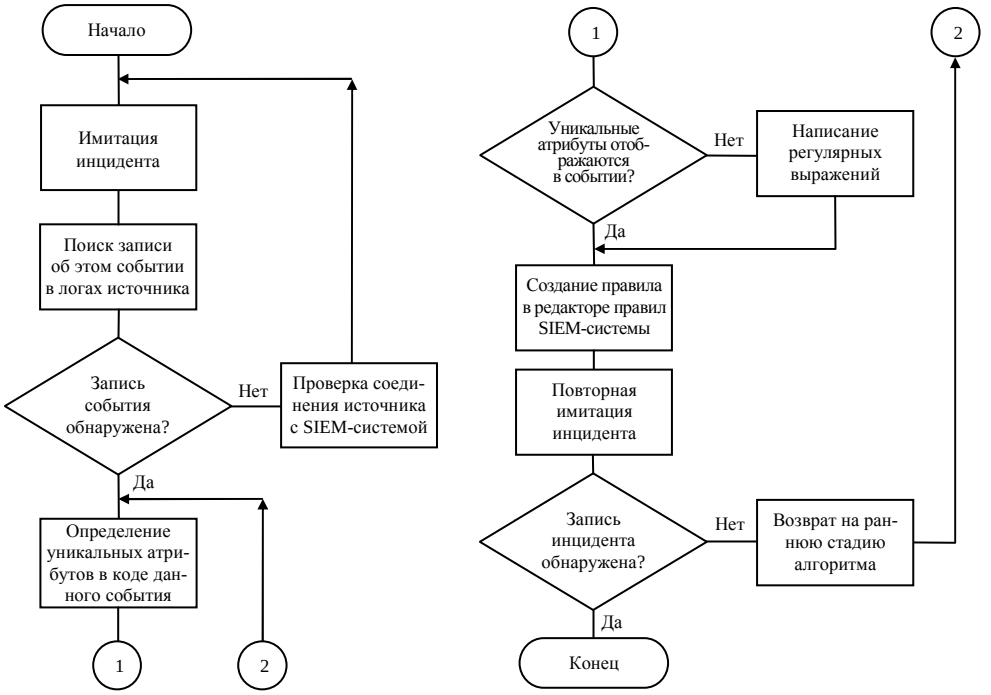

Рис. 3. Схема алгоритма написания правила

Регулярное выражение «proto=(.?)\» выделяет часть кода после «proto=» до следующего специального символа. В данной части кода записывается название протокола (рис. 4).

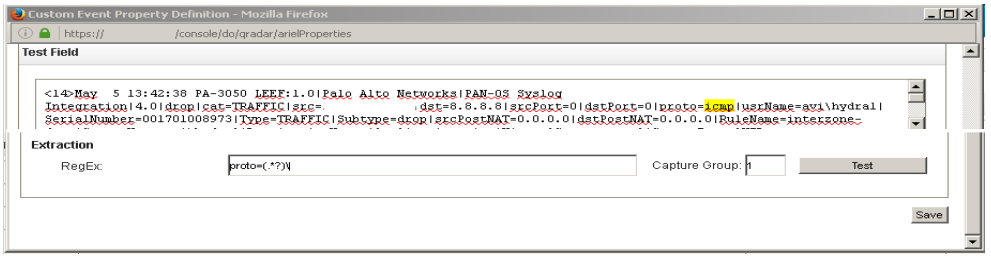

Рис. 4. Создание правила выделения свойства через «регулярное выражение»

Теперь в свойствах события указывается протокол (рис. 5).

Следующим шагом является создание правила в редакторе QRadar. В данном редакторе можно выбирать условия срабатывания правила. При этом чем больше подобных условий, тем меньше ложных срабатываний системы.

Для данного правила были выбраны следующие условия (рис. 6):

Event Information

Event Name	Session Denied - No Allow Rule or Port Based Deny Rule						
Low Level Category	Access Denied						
Event Description	Session denied due to no allow rule or port-based deny rule						
Magnitude	(8)	**Relevance**	10	**Severity**	4	**Credibility**	10
Username	avi\hydra1						
Start Time	May 6, 2016, 12:52:18 AM	**Storage Time**	May 6, 2016, 12:52:18 AM	**Log Source Time**	May 6, 2016, 12:52:27 AM		
Network protocol (custom)	tcp						
PA signature name (custom)	N/A						
PA_ACTION (custom)	N/A						
PA_URL (custom)	N/A						
PA_category (custom)	TRAFFIC						
PA_signature_name (custom)	N/A						
PA_subtype (custom)	N/A						
pa_destination_zone (custom)	MTS-INET						
pa_severity (custom)	N/A						
pa_source_zone (custom)	AVID-LAN						

Рис. 5. Проверка работоспособности регулярного выражения

– данное событие было обнаружено на межсетевом экране;
– IP источника находится в определенной группе;
– имя протокола из списка: «icmp, tcp, udp».

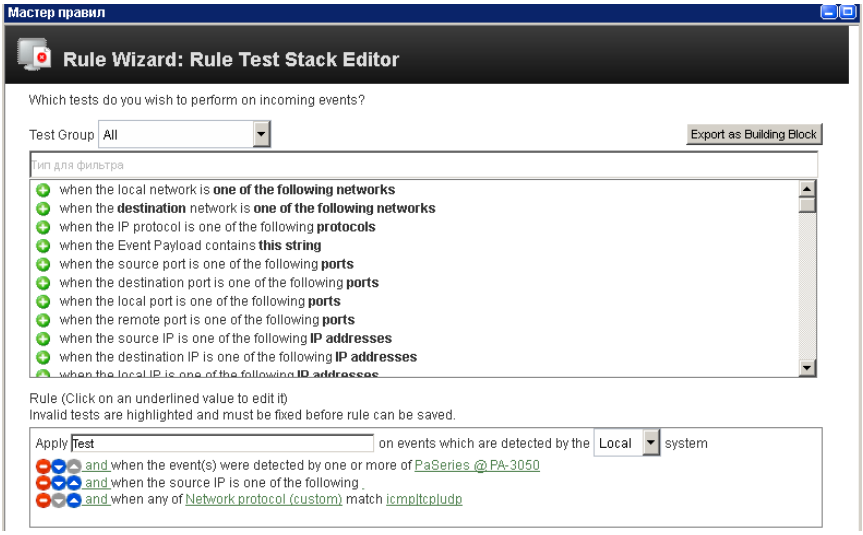

Рис. 6. Создание правила в редакторе

Следующим пунктом настройки правила является настройка свойств инцидента, генерируемого при срабатывании правила. В данных настройках можно указать название инцидента, аннотацию к инциденту, группу, в которую входит это правило, степень критичности данного инцидента [9].

Таким образом, защита информации представляет собой непрерывный целенаправленный процесс, продолжающийся на всем жизненном цикле информационной системы. Поэтому важно постоянно модифицировать и дорабатывать систему защиты информации и его компонентов в частности. Внедрение и последующее совершенствование SIEM-системы позволяют повысить уровень защищенности информации в информационной системе [10]. Кроме того, SIEM-система существенно облегчает работу по администрированию и управлению безопасностью любого предприятия и организации за счет сохранения информации об инциденте, возможности определения ответственного за обработку конкретного инцидента, а также сроков обработки инцидента. В свою очередь, собранные и обработанные статистические данные позволяют судить об эффективности работы, как отдельных средств защиты информации, так и системы безопасности в целом.

Библиографический список

1. Шабуров А.С., Борисов В.И. О применении сигнатурных методов анализа информации в SIEM-системах // Вестник УрФО. Безопасность в информационной среде. – Челябинск: Изд. центр ЮУрГУ, 2015. – № 17. – С. 23–37.

2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Доступ из справ.-правовой системы КонсультантПлюс.

3. Факторы, влияющие на организацию КСЗИ [Электронный ресурс]. – URL: http://webkonspect.com/?id=6547&labelid=60637&room=profile (дата обращения: 27.04.2016).

4. Алексей Дрозд, Обзор SIEM-систем. SearchInform [Электронный ресурс]. – URL: http://www.antimalware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market (дата обращения: 27.04.2016).

5. SIEM-системы. Инфобезпека [Электронный ресурс]. – URL: http://www.infobezpeka.com/publications/SIEM_osobennosti_siem (дата обращения: 27.04.2016).

6. Панасенко А. Основные возможности SIEM, исследовательский центр Anti-Malware [Электронный ресурс]. – 2015. – URL: https://www.anti-malware.ru/reviews/SearchInfrom_dlp_SIEM (дата обращения: 27.04.2016).

7. Кузнецов А., Федоров А. Современные тенденции развития SIEM-решений, «StorageNews». – № 2(54) [Электронный ресурс]. – URL: http://www.ntc-vulkan.ru/images/stories/publication/Vulkan_IS_54-9_final.pdf (дата обращения: 27.04.2016).

8. Способы резервного копирования файлов [Электронный ресурс]. – URL: http://windows.microsoft.com/ru-ru/windows/methods-of-backing-upyour-files (дата обращения: 27.04.2016).

9. Жизненный цикл информационных систем. Студопедия [Электронный ресурс]. – URL: http://studopedia.ru/3_9104_lektsiya--zhiznenniy-tsikl-informatsionnih-sistem.html (дата обращения: 27.04.2016).

10. Шабуров А.С., Борисов В.И. О применении SIEM-систем для обеспечения безопасности корпоративных сетей // Инновационные технологии, теория, инструменты, практика: материалы VII Междунар. интернет-конф. молод. ученых, аспирант., студентов. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2015. – С. 249–254.

References

1. Shaburov A.S., Borisov V.I. O primenenii signaturnykh metodov analiza informatsii v SIEM-sistemakh [Application of information signature testing in SIEM-systems]. Vestnik Ural'skogo federal'nogo okruga. Bezopasnost' v informatsionnoi srede. Cheliabinsk: Izdatel'skii tsentr Iuzhno-Ural'skogo gosudarstvennogo universiteta, 2015, no. 17, pp. 23-37.

2. Ob informatsii, informatsionnykh tekhnologiiakh i o zashchite informatsii: Federal'nyi zakon ot 27 July 2006. № 149-FZ [Information, information technologies and information security: Federal Law dated by 27 July 2006. № 149-ФЗ]. Dostup iz spravochno-pravovoi sistemy Konsul'tantPlius.

3. Faktory, vliiaiushchie na organizatsiiu KSZI [Factors, influencing the arrangement of integrated information security systems], available at: http://webkonspect.com/?id=6547&labelid=60637&room=profile (accessed 27 April 2016).

4. Drozd A. Obzor SIEM-sistem. SearchInform [Review of SIEM-systems. SearchInform], available at: http://www.antimalware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market (accessed 27 April 2016).

5. SIEM-sistemy. Infobezpeka [SIEM-systems. Infobezpeka], available at: http://www.infobezpeka.com/publications/SIEM_osobennosti_siem (accessed 27 April 2016).

6. Panasenko A. Osnovnye vozmozhnosti SIEM, issledovatel'skii tsentr Anti-Malware [The main SIEM capabilities, research center Anti-Malware], 2015, available at: https://www.anti-malware.ru/reviews/ SearchInfrom_dlp_SIEM (accessed 27 April 2016).

7. Kuznetsov A., Fedorov A. Sovremennye tendentsii razvitiia SIEM-reshenii, "StorageNews" [Modern tendency of the SIEM-decision development, «StorageNews»], no. 2(54), available at: http://www.ntc-vulkan.ru/images/ stories/publication/ Vulkan_IS_54-9_final.pdf (accessed 27 April 2016).

8. Sposoby rezervnogo kopirovaniia failov [Back-up files method], available at: http://windows.microsoft.com/ru-ru/windows/methods-of-backing-upyour-files (accessed 27 April 2016).

9. Zhiznennyi tsikl informatsionnykh sistem. Studopediia [Information system life cycle. Studopedia], available at: http://studopedia.ru/3_9104_lektsiya--zhiznenniy-tsikl-informatsionnih-sistem.html (accessed 27 April 2016).

10. Shaburov A.S., Borisov V.I. O primenenii SIEM-sistem dlia obespecheniia bezopasnosti korporativnykh setei [Application the SIEM-systems for safety and security arrangement of corporate]. *Materialy VII Mezhdunarodnoi internet-konferentsii molodykh uchenykh, aspirantov, studentov «Innovatsionnye tekhnologii, teoriia, instrumenty, praktika». Permskii natsional'nyi issledovatel'skii politekhnicheskii universitet*, 2016, pp. 249-254.

Сведения об авторах

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.ru).

Борисов Владислав Игоревич (Пермь, Россия) – студент Пермского национального исследовательского политехнического университета (614097, Пермь, Комсомольский пр., 29, e-mail: borisovvi94@yandex.ru).

About the authors

Shaburov Andrey Sergeevich (Perm, Russian Federation) is a Ph.D. in Technical Sciences, Associate Professor of the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: shans@at.pstu.ru).

Borisov Vladislav Igorevich (Perm, Russian Federation) is a Student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: borisovvi94@yandex.ru).

Получено 14.07.2016