www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.2.6

УДК 004.056.53
ББК 65.422

# СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

**Александр Сергеевич Родионов**

Кандидат технических наук, доцент кафедры информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова
RAS001m@mail.ru
ул. Просвещения, 132, 346428 г. Новочеркасск, Российская Федерация

**Владислав Игоревич Белянин**

Магистр кафедры информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова
vbeluev@mail.ru
ул. Просвещения, 132, 346428 г. Новочеркасск, Российская Федерация

**Александр Андреевич Горбунов**

Магистр кафедры информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова
kent1157@bk. ru
ул. Просвещения, 132, 346428 г. Новочеркасск , Российская Федерация

**Аннотация.** Актуальность работы обусловлена постоянно растущими техническими возможностями по несанкционированному доступу к защищаемой информации в ЛВС, развитию способов проведения атак, следовательно необходимостью совершенствования методов защиты информации. В работе рассмотрены особенности использования системы сбора и корреляции событий информационной безопасности SIEM (Security Information and Event Management), которая выявляет угрозы утечки защищаемой информации и оповещает об их появлении.

**Ключевые слова:** защита информации, несанкционированный доступ, программные средства защиты, система SIEM, эффективность защиты информации.



В современном мире в связи с постоянно растущими техническими возможностями злоумышленников по несанкционированному доступу к защищаемой информации в локальных вычислительных сетях (ЛВС), совершенствованию способов проведения на них атак возникает необходимость совершенствования известных и разработки новых методов защиты информации.

Помимо технической составляющей немаловажным фактором риска является «человеческий», из-за которого по всему миру

происходит до 52 % утечек информации (преднамеренных и непреднамеренных). Они распределяются по следующим категориям: 62,3 % – персональные данные, 31,0 % – платежные документы, 3,9 % – государственные тайны, 2,8 % – коммерческие тайны [4].

Необходимость защиты информации, содержащейся в информационных системах, в том числе государственных (ГИС), устанавливает Федеральный Закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В данном документе указывается на то, что «лица, владеющие информацией, а также занимающиеся непосредственно обработкой (операторы ИС), обязаны обеспечивать должную защиту информации путем принятия организационных, технических и правовых мер, направленных на соблюдение таких трех составляющих, как конфиденциальность, целостность и доступность» [5].

Организация, занимающаяся обработкой защищаемой информации, обязана выполнять следующие задачи:

– контроль функционирования системы защиты;

– непрерывное совершенствование средств и методов контроля над работоспособностью механизмов защиты;

– совершенствование методов борьбы с вредоносными программами и вирусами;

– оптимизацию затрат на создание и эксплуатацию систем контроля, выражающуюся в экономической целесообразности применения систем информационной безопасности.

Реализация перечисленных задач предполагает использование соответствующих методов и средств защиты информации.

Программные, технические, программно-аппаратные являются одними из основных средств, которые обеспечивают безопасность в современных информационных системах.

Эффективными способами защиты считаются криптографические средства. Те из них, которые удовлетворяют соответствующим требованиям, характеризуются наибольшей надежностью и основываются на всевозможных криптоалгоритмах для шифрования данных [2].

Систематическое применение всех перечисленных выше средств и методов современной защиты информации значительно увеличивает надежность системы безопасности и предотвращает разглашение защищаемой информации.

При этом существующие методы защиты информации включают в себя довольно большое количество механизмов и являются весьма трудоемким процессом, требующим постоянного совершенствования и оптимизации.

Рассмотрим один из них, а именно совершенствование программных средств защиты от несанкционированного доступа (НСД).

Выделим относительно новую, но малоизвестную в нашей стране систему сбора и корреляции событий информационной безопасности (ИБ) *SIEM*, которая относится к программным средствам.

Система защиты информации организации состоит из множества составляющих: антивирусные программы, межсетевые экраны, *DLP*, *Web*, *E-mail*-фильтрации и другие решения. Отдельные элементы защиты, пусть даже и лучшие в данном классе, имеют разные стандарты представления информации, что усложняет мониторинг событий ИБ, их сравнение, выявление и расследование.

Для оперативного обнаружения и реагирования на события ИБ современных предприятий используют системы класса *SIEM (Security Information and Event Management)*. *SIEM* – это средство для автоматизации процессов выявления и реагирования на события в системе ИБ. Последняя выполняет сбор и анализирует события ИБ, в результате чего обнаруживает угрозы утечки защищаемой информации и оповещает об их появлении [6].

Стандартом построения системы является *ISO* 17799, который предусматривает внедрение комплексного подхода к решению поставленных задач по обеспечению конфиденциальности, целостности и доступности данных.

Данная система может функционировать в комплексе как с интегрированной, так и с адаптивной системой управления безопасностью.

Работа *SIEM* заключается в том, что система получает информацию о событиях из

таких источников, как межсетевые экраны, IPS, антивирусные программы, операционные системы (ОС), накопители и т. д. Она отфильтровывает приобретенную информацию, приводя ее к единому формату. Это позволяет формировать и централизованно сохранять журналы событий. Далее *SIEM* отлаживает события: находит взаимосвязи и закономерности, что позволяет с высокой точностью выявлять потенциальные угрозы, аномалии, сбои в работе информационной системы, попытки несанкционированного доступа. Кроме того, использование SIEM дает возможность автоматизировать процессы реагирования на всевозможные инциденты ИБ.

В таблице приведены некоторые проблемы, которые можно решить *SIEM* системой. Ее использование позволит повысить эффективность защиты информации от НСД:

– снизить возникновение угроз ИБ за счет оперативного выявления и своевременного реагирования;

– сократить затраты и повысить производительность работы персонала;

– автоматизировать процесс оценки угроз и уязвимостей в соответствии с требованиями отечественных и зарубежных стандартов;

– эффективно контролировать состояние информационной системы и сократить время возможных задержек;

– оценивать эффективность имеющихся средств защиты информации за счет выявления и локализации всевозможных инцидентов ИБ;

– централизованно хранить информацию о процессах и инцидентах информационной безопасности с возможностью их последующего анализа.

Таким образом, к перспективным, но пока мало распространенным защитным технологиям от НСД можно отнести SIEM, PKI системы корреляции событий безопасности и системы единого управления разнородными средствами защиты. Данные технологии в настоящее время востребованы только в случаях комплексного применения межсетевых экранов, антивирусов, систем разграничения доступа, контроля НСД и т. д. Лишь десятки из тысяч российских компаний используют такие комплексные системы защиты информации [1; 3].

Применение данных технологий позволит в значительной степени уменьшить факторы риска по НСД, нарушения работы ИС и тем самым приведет к стабильности работы организации в целом.

### *СПИСОК ЛИТЕРАТУРЫ*

1. Домбровская, Л. А. Современные подходы к защите информации, методы, средства и инст-

**Проблемы сторонних систем защиты информации и их решение с использованием технологии SIEM**

| Проблемы сторонних систем защиты информации | Решение проблем с использованием *SIEM* систем |
|---|---|
| Значимое количество информационных систем и средств защиты информации создает огромные объемы журналов событий, непригодных для анализа | *SIEM* дает возможность осуществлять сбор событий практически с любых источников, приводя их к единообразному виду, пригодному для последующего анализа |
| Часто возникают ситуации, когда в потоке данных находятся повторяющиеся события, которые добавляют объем и мешают анализу, при этом их нельзя игнорировать | *SIEM* позволяет агрегировать однотипные события, давая возможность использовать их при анализе ситуации, при этом они не размывают общую картину происходящего |
| Для обнаружения сложных атак, цепочек событий требуется сопоставлять события из разных систем в режиме реального времени, что невозможно реализовать в ручном режиме | Решения класса *SIEM* позволяют автоматизировать процесс сопоставления событий между собой по критериям, давая возможность в автоматическом режиме обнаруживать сложные для выявления инциденты |
| Хранение журналов событий различных информационных систем является сложным процессом для анализа и расследований, что может оказаться невозможным из-за технических ограничений данных систем | *SIEM* осуществляет сбор событий с источников и позволяет хранить их установленное количество времени, при этом использует сжатие и решает задачу централизованного архивного хранения |

румenты защиты / Л. А. Домбровская, Н. А. Яковлева, Р. Е. Стахно. – Электрон. текстовые дан. – Режим доступа: https://www.3minut.ru (дата обращения: 10.11.2017). – Загл. с экрана.

2. Кияев, В. И. Безопасность информационных систем / В. И. Кияев, О. Н. Граничин. – М. : Открытый Университет «ИНТУИТ», 2016. – 192 с.

3. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия / В. В. Баранов, М. А. Коцыняк, О. С. Лаута, В. М. Московченко // Вестник Волгоградского государственного университета. Серия 10, Инновационная деятельность. – 2017. – Т. 11, № 2. – С. 11–15.

4. Развитие информационных угроз в 2017 году / Р. Унучек, Ф. Синицын, Д. Паринов, А. Лискин. – Электрон. текстовые дан. – Режим доступа: https://securelist.ru/it-threat-evolution-q2-2017-statistics/79226/ (дата обращения: 03.11.2017). – Загл. с экрана.

5. Российская Федерация. Законы. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – Доступ из справ.-правовой системы «КонсультантПлюс».

6. Современные системы защиты информации от НСД // Компания «Инфозащита». – Электрон. текстовые дан. – Режим доступа: http://itprotect.ru (дата обращения: 09.11.2017). – Загл. с экрана.

### *REFERENCES*

1. Dombrovskaya L.A., Yakovleva N.A., Stakhno R.E. *Sovremennye podkhody k zashchite informatsii, metody, sredstva i instrumenty zashchity* [Modern Approaches to Data Protection, Methods, Means and Tools of Protection]. URL: https://www.3minut.ru (accessed 10 November 2017).

2. Kiyaev V., Granichin O. *Bezopasnost informatsionnykh sistem* [Security of Information Systems]. Moscow, INTUIT Publ., 2016. 192 p.

3. Baranov V.V., Kotsynyak M.A., Lauta O.S., Moskovchenko V.M. Metodika otsenki ustoychivosti informatsionno-telekommunikatsionnoy seti v usloviyakh informatsionnogo vozdeystviya [Estimating Sustainability of Telecommunication Networks in Terms of Information Influence]. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 10: Innovatsionnaya deyatelnost* [Science Journal of Volgograd State University. Innovation Technology], 2017, vol. 11, no. 2, pp. 11-15.

4. Unuchek R., Sinitsyn F., Parinov D., Liskin A. *Razvitie informatsionnyh ugroz v 2017 godu* [Development of Information Threats in 2017]. URL: https://securelist.ru/it-threat-evolution-q2-2017-statistics/79226/. (accessed 3 November 2017).

5. *Rossiyskaya Federatsiya. Zakony. Federalnyy zakon ot 27.07.2006 № 149-FZ «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii»* [The Russian Federation. Laws. Federal Law of 27 July 2006 No. 149-FL 'On Information, Information Technologies and Information Protection]. URL: http://www.consultant.ru (accessed 3 November 2017).

6. Sovremennye sistemy zashchity informatsii ot NSD [Modern Systems of Information Protection from Unauthorized Access]. *Kompaniya «Infozashchita»* [Infozashchita Company]. URL: http://itprotect.ru (accessed 9 November 2017).

## IMPROVING THE METHODS FOR PROTECTING INFORMATION FROM UNAUTHORIZED ACCESS

**Aleksandr S. Rodionov**

Candidate of Sciences (Engineering),
Associate Professor, Department of Information Security,
South-Russian State Polytechnic University named after M.I. Platov
RAS001m @mail.ru
Prosveshcheniya St., 132, 346428 Novocherkassk, Russian Federation

**Vladislav I. Belyanin**

Master Student, Department of Information Security,
South-Russian State Polytechnic University named after M.I. Platov
vbeluev@mail.ru
Prosveshcheniya St., 132, 346428 Novocherkassk, Russian Federation

**Aleksandr A. Gorbunov**

Master Student, Department of Information Security,
South-Russian State Polytechnic University named after M.I. Platov
kent1157@bk. ru
Prosveshcheniya St., 132, 346428 Novocherkassk, Russian Federation

**Abstract.** The research relevance is conditioned by the constantly growing technical capabilities for unauthorized access to protected information in the local area networks (LAN), the development of methods of attacks, and therefore, the need to improve methods of information protection. The paper describes the peculiarities of using the system of collecting and correlating information security events SIEM (Security Information and Event Management), which detects and notifies about the emergence of threats to leakage of protected information.

In the modern world, due to the ever-growing technical capabilities of attackers for unauthorized access to LAN, improving the ways of carrying out attacks on them, there is a need to improve the existing methods of information protection and to develop new ones.

In addition to the technical component, an important risk factor is the human factor, due to which up to 52 % of information leaks (intentional and unintended) occur around the world. They are distributed by categories of information: 62.3 % – personal data, 31.0 % – payment documents, 3.9 % – state secrets, 2.8 % – trade secrets.

**Key words:** data protection, unauthorized access, software protection, SIEM system, efficiency of information protection.