СИСТЕМНЫЙ АНАЛИЗ И УПРАВЛЕНИЕ
SYSTEM ANALYSIS AND PROCESSING OF KNOWLEDGE

УДК 681.518
DOI 10.52575/2687-0932-2021-48-1-116-122

Подход к разработке системы выявления инцидентов информационной безопасности информационных ресурсов банковских систем при реализации этапов противодействия противоправным действиям

Александров В.В., Малий Ю.В., Александрова Ю.В., Семенякин А.И.
Белгородский университет кооперации, экономики и права,
Россия, 308023, г. Белгород, ул. Садовая, 116а
E-mail: kaf-otzi@bukep.ru

Аннотация. Целью данной статьи является рассмотрение подхода к определению вероятности выявления инцидентов информационной безопасности информационных ресурсов банковских систем, при реализации этапов противодействия противоправным действиям (НСД, копирование, изменение, уничтожение информации). Авторами рассмотрена актуальность применения системы Security Information and Event Management (SIEM). Описаны источники данных для систем выявления инцидентов, атрибуты, которые могут быть проанализированы SIEM системой. При рассмотрении подхода к определению вероятности выявления инцидентов информационной безопасности введены параметры v_n, $v_{(min)}$ обозначающие объем и минимальный объем базы правил корреляции системы выявления инцидентов информационной безопасности соответственно. Как результат определена вероятность, позволяющая полно характеризовать систему выявления инцидентов информационной безопасности информационных ресурсов банковских систем, при реализации этапов противодействия противоправным действиями (НСД, копирование, изменение, уничтожение информации).

Ключевые слова: информационная безопасность, банковские информационные ресурсы, выявление инцидентов информационной безопасности, правила корреляции, система выявления инцидентов информационной безопасности.

Для цитирования: Александров В.В., Малий Ю.В., Александрова Ю.В., Семенякин А.И. 2021. Подход к разработке системы выявления инцидентов информационной безопасности информационных ресурсов банковских систем при реализации этапов противодействия противоправным действиям. Экономика. Информатика, 48 (1): 116–122. DOI: 10.52575/2687-0932-2021-48-1-116-122.

Approach to development of a system for detecting incidents of information security of information resources of banking systems, when implementing stages of counteraction of illegal actions

Vitaliy V. Aleksandrov, Yuliya V. Maliy, Yuliya V. Aleksandrova, Aleksandr I. Semenyakin
Belgorod University of Cooperation, Economics and Law, Russia,
116A Sadovaya St, Belgorod, 308023, Russia
E-mail: kaf-otzi@bukep.ru

Abstract. The purpose of this article is to consider an approach to determining the probability of detecting information security incidents of information resources of banking systems, when implementing the stages of countering illegal actions (unauthorized actions, copying, changing, destroying information). The authors

considered the relevance of using the Security Information and Event Management (SIEM) system. The data sources for incident detection systems, attributes that can be analyzed by the SIEM system are described. When considering an approach to determining the probability of detecting information security incidents, the parameters vn, v (min) were introduced, denoting the volume and minimum volume of the correlation rule base of the information security incident detection system, respectively. As a result, the probability was determined, which makes it possible to fully characterize the system for identifying incidents of information security of information resources of banking systems when implementing the stages of countering illegal actions (unauthorized actions, copying, changing, destroying information).

Keywords: information security, banking information resources, identification of information security incidents, correlation rules, information security incident detection system.

For citation: Alexandrov V.V., Maliy Yu.V., Alexandrova Yu.V., Semenyakin A.I. 2021. Approach to development of a system for detecting incidents of information security of information resources of banking systems, when implementing stages of counteraction of illegal actions. Economics. Information technologies, 48 (1): 116–122 (in Russian). DOI: 10.52575/2687-0932-2021-48-1-116-122.

Введение

При построении системы защиты информации число источников, отражающих актуальную защищенность, непрерывно растет, возрастает нагрузка на администраторов безопасности, что ведет к несвоевременному выявлению угроз безопасности и делает уязвимой систему защиты [Заряев, 2003; Малюк, 2004; Хорев, 2008; Пономаренко и др., 2018]. Проблема защиты банков от хакерских атак обсуждалась на конференции «SIEM в банковской сфере: автоматизация хаоса», организованной журналом «Банковское обозрение». За последние 5 лет произошел резкий рост крупномасштабных, скоординированных и хорошо организованных хакерских атак на банки, ставящих под угрозу экономическую стабильность, сохранность финансовых активов, безопасность персональных данных и корпоративной конфиденциальной информации, поэтому в предотвращении таких неприятных инцидентов заинтересованы как банки, так и их клиенты.

Участники конференции сошлись на том, что на сегодняшний день SIEM – это некий технологический минимум, который обязательно должен быть у каждого банка.

С целью комплексной защиты финансовые учреждения активно внедряют в использование комбинированное программное обеспечение по управлению событиями информационной безопасности, получившее аббревиатуру SIEM: от SIM, security information management – управление информационной безопасностью и от SEM, security event management – управление событиями безопасности. Его суть – собирать информацию о событиях, мониторить сетевой трафик, действия пользователей и неопознанных устройств, анализировать инциденты [Официальный сайт системы NetIQ Sentinel SIEM, дата обращения 15.10.2020].

Основная часть

Работа SIEM системы построена по принципу объединения данных о событиях из разных источников в сетевой инфраструктуре, включая серверы, системы, устройства и приложения, от периметра до конечного пользователя, в конечном счете, решение SIEM анализирует данные на предмет отклонений от правил поведения, определенных организацией, для выявления потенциальных угроз (рис. 1).

Источниками данных для систем выявления инцидентов являются [Официальный сайт системы MaxPatrol SIEM, дата обращения 15.10.2020]:

1. Сетевые устройства: маршрутизаторы, коммутаторы, мосты, точки беспроводного доступа, модемы, линейные драйверы, концентраторы.
2. Серверы: веб, прокси, почта, FTP.
3. Устройства безопасности: IDP / IPS, брандмауэры, антивирусное программное обеспечение, устройства фильтрации контента, устройства обнаружения вторжений.
4. Приложения: любое программное обеспечение, используемое на любом из перечисленных устройств.

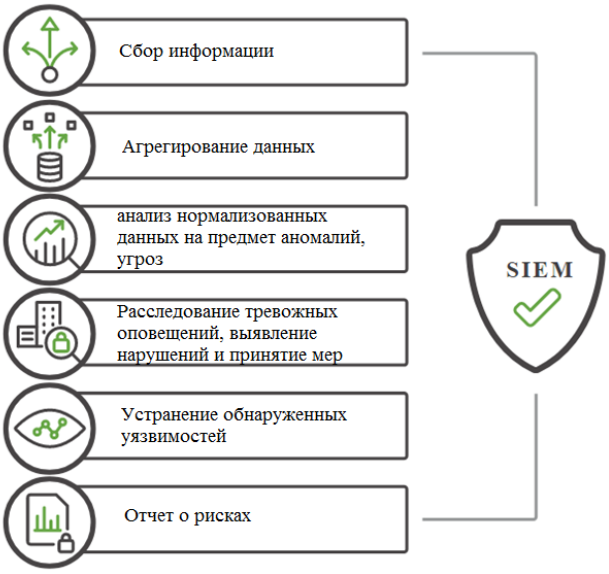

Рис. 1. Работа SIEM системы
Fig. 1. SIEM system operation

Атрибуты, которые могут быть проанализированы, включают пользователей, типы событий, IP-адреса, память, процессы и многое другое [Авсентьев, 2016]. Эта информация передается на консоль управления, где анализируется для устранения возникающих угроз. Как только необходимая информация попадает в консоль управления, она просматривается администратором безопасности, который может предоставить обратную связь по всему процессу. Обратная связь помогает обучить систему SIEM с точки зрения машинного обучения и повышения ее знакомства с окружающей средой. Как только программная система SIEM идентифицирует угрозу, она связывается с другими системами безопасности на устройстве, чтобы остановить нежелательную деятельность [Miller, 2010].

Каждый пользователь или устройство оставляет за собой виртуальный след в журналах устройств [Пономаренко и др., 2017]. Системы SIEM используют данные этих журналов, чтобы получить информацию о произошедших атаках и событиях. SIEM не только идентифицирует, что атака произошла, но и позволяет увидеть, как и почему она произошла, что позволяет повысить экономическую стабильность, сохранность финансовых активов, безопасность персональных данных и корпоративной конфиденциальной информации [Официальный сайт системы ViPNet TIAS, дата обращения 15.10.2020].

Результаты и их обсуждение

В работе рассматривается подход к определению вероятности выявления инцидентов информационной безопасности информационных ресурсов банковских систем, при реализации этапов противодействия противоправным действиями (НСД, копирование, изменение, уничтожение информации).

Были введены следующие понятия:

v_n – объем базы правил корреляции системы выявления инцидентов информационной безопасности;

$v_{(min)}$ – минимальный объем базы правил корреляции системы выявления инцидентов информационной безопасности.

v_c – объем базы правил корреляции системы выявления инцидентов информационной безопасности в реализующих с-ю функцию.

Тогда при осуществлении *n*-го этапа противоправных действий в отношении банковских информационных ресурсов можно представить следующее выражение, показывающее, что инцидент информационноой безопасности будет выявлен при условии когда объем базы правил корреляции системы выявления инцидентов информационной безопасности не менее минимально

допустимой величины $t_{(\min)\,n}$ [Александров, 2010; Авсентьев, Авсентьев, 2015; Авсентьев и др., 2015; Меньших, Авсентьев, 2015; Авсентьев, Жидко, 2016; Авсентьев и др., 2016; Скрыль и др., 2017]:

$$v_n \geq v_{(\min)\,n}\,. \tag{1}$$

Так как v_n является функцией от характеристик системы выявления инцидентов информационной безопасности, выполняющих определенные направления защиты, то:

$$v_n = \sum_{m=1}^{M} \circ\, t_c\,, \tag{2}$$

где v_c – объем базы правил корреляции системы выявления инцидентов информационной безопасности, реализующих m-ое направление защиты, а операция $\sum_{m=1}^{M} \circ$ означает композицию M случайных величин.

Входящая в (1) величина v_e является случайной [Скрыль, Мишин, 2005; Скрыль и др., 2010; Авсентьев и др., 2016]:

$$P = P(v_e \geq v_{(\min)e})\,. \tag{3}$$

Данную вероятность можно описать как среднее количество событий, когда инцидент был включен в базу правил корреляции и распознан системой выявления инцидентов информационной безопасности в рамках n-го этапа противоправных действий, относительно общего числа инцидентов:

$$P = P(v_n \geq v_{(\min)n}) = \frac{1}{G}\sum_{g=1}^{G}\delta_{n,g}\,, \tag{4}$$

где $\delta_{eg} = \begin{cases} 1, \ при\ v_{ng} \geq v_{(\min)ng} \\ \\ 0, \ при\ v_{ng}^{(2)} < v_{(\min)ng} \end{cases}$;

v_{eg} – объем базы правил корреляции системы выявления инцидентов информационной безопасности, реализующих n-й этап противодействия g-й, g = 1, 2, …, G, угрозе противоправных действий;

$v_{(\min)\,cg}$ – минимальный объем базы правил корреляции системы выявления инцидентов информационной безопасности, соответствующий g-ой угрозе при реализации n-го этапа мероприятий по защите информации;

G – общее число исследуемых инцидентов информационной безопасности в отношении информационных ресурсов банковских систем.

В связи с тем, что в (1) изменяемым параметром может являться минимальный объем базы правил корреляции системы выявления инцидентов информационной безопасности, вероятность (2) может быть записана так:

$$P_n = P(v_n \geq v_{(\min)n}) = 1 - P(v_e < v_{(\min)n}), n = 1,2,\ldots,N\,. \tag{5}$$

Указанная вероятность позволяет полно характеризовать систему выявления инцидентов информационной безопасности информационных ресурсов банковских систем, при реализации этапов противодействия противоправным действиями (НСД, копирование, изменение, уничтожение информации).

Заключение

В ходе исследования была определена вероятность, позволяющая полно характеризовать систему выявления инцидентов информационной безопасности информационных ресурсов банковских систем, при реализации этапов противодействия противоправным действиям таким как НСД, копирование, изменение, уничтожение информации.

Список источников

1. Официальный сайт системы MaxPatrol SIEM. URL: https://www.ptsecurity.com/ru-ru/products/mpsiem/ (дата обращения 15.10.20).

2. Официальный сайт системы NetIQ Sentinel SIEM. URL: https://www.netiq.com/products/sentinel/ (дата обращения 15.10.20).

3. Официальный сайт системы ViPNet TIAS. URL: https://infotecs.ru/product/vipnet-tias.html (дата обращения 15. 10.20).

Список литературы

1. Авсентьев А.О. 2016. Определение ценности информации, ТУСУР. 19 (1): 21–24.

2. Авсентьев О.С. Авсентьев А.О. 2015. Формирование обобщенного показателя ценности информации в каналах связи. Вестник Воронежского института МВД России. 2: 55–63.

3. Авсентьев О.С. Вальде А.Г., Кругов А.Г. 2016. Математическая модель защиты информации от утечки по электромагнитным каналам. Вестник Воронежского института МВД России. 3: 42–50.

4. Авсентьев О.С. Жидко Е.А. 2016. Обоснование требований к уровню информационной безопасности объекта защиты. Вестник Воронежского института МВД России. 1: 33–43.

5. Авсентьев О.С. Меньших В.В., Авсентьев А.О. 2015. Моделирование и оптимизация процессов передачи и защиты информации в каналах связи. Специальная техника. 5: 47–50.

6. Авсентьев О.С. Меньших В.В., Авсентьев А.О. 2016. Модель оптимизации процесса передачи информации по каналам связи в условиях угроз ее безопасности. Телекоммуникации. 1: 28–32.

7. Александров В.В. 2010. Показатели эффективности реализации информационных процессов в ИТКС в условиях противодействия угрозам информационной безопасности. В кн.: Теория и практика инновационного развития кооперативного образования и науки. Белгород, Издательство БУКЭП: 18–20.

8. Заряев А.В. 2003. Источники и каналы утечки информации в телекоммуникационных системах. Воронеж, Воронежский институт МВД России, 305.

9. Малюк А.А. 2004. Информационная безопасность: концептуальные и методологические основы защиты информации. М., Горячая линия Телеком, 280.

10. Меньших В.В., Авсентьев А.О. 2015. Модель оптимизации процесса обеспечения требований к свойствам информации при ее передаче по каналам связи. Вестник Воронежского института МВД России. 4: 147–154.

11. Пономаренко С.В., Пономаренко С.А., Александров В.В. 2017. Моделирование несанкционированного доступа к информационным ресурсам ключевых систем информационной инфраструктуры. Белгород, Издательство БУКЭП, 177.

12. Пономаренко С.В., Прокушев Я.Е., Александров В.В., Ломазов В.А. 2018. Актуальные проблемы экономической безопасности персональных данных информационных инфраструктур банковской сферы. Вестник Белгородского университета кооперации, экономики и права. 4: 246–252.

13. Скрыль С.В., Мишин Д.С. 2005. Угрозы информационной безопасности в компьютерных сетях органов внутренних дел. В кн.: Современные проблемы борьбы с преступностью. Воронеж, Воронежский институт МВД России, 5–6.

14. Скрыль С.В., Спивак В.И., Щербаков А.В., Пономаренко С.В. 2017. Проблема оптимизации процедур комплексного технического контроля защищенности информации от утечки по каналам ПЭМИН: концепция решения. Телекоммуникации. М., Наука и технологии ООО, 10: 23–34.

15. Скрыль С.В., Финько В.Н., Пономаренко С.В., Волкова С.Н., Рябинин Г.И. 2010. Показатель эффективности информационной деятельности органов государственного управления в условиях противодействия утечке информации по техническим каналам Информация и безопасность. 13 (1): 141–142.

16. Хорев А.А. 2008. Техническая защита информации: Т. 1. Технические каналы утечки информации. М., НПЦ «Аналитика», 436.

17. Miller D., Harris S., Harper S., VanDyke C. 2010. Security Information and Event Management (SIEM) Implementation. McGraw Hill Professional, 464 p.

References

1. Avsentiev A.O. 2016. Determining the value of information, TUSUR. 19 (1): 21–24. (in Russian)

2. Avsentiev O.S. Avsentiev A.O. 2015. Formation of a generalized indicator of the value of information in communication channels. Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2: 55–63. (in Russian)

3. Avsentiev O.S. Walde A.G., Krugov A.G. 2016. Mathematical model of information protection against leakage through electromagnetic channels. Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 3: 42–50. (in Russian)

4. Avsentiev O.S. Zhidko E.A. 2016. Justification of requirements for the level of information security of the protected object. Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 1: 33–43. (in Russian)

5. Avsentiev O.S. Menshikh V.V., Avsentiev A.O. 2015. Modeling and optimization of information transmission and protection processes in communication channels. Special equipment. 5: 47–50. (in Russian)

6. Avsentiev O.S. Menshikh V.V., Avsentiev A.O. 2016. A model for optimizing the process of transferring information through communication channels in conditions of threats to its security. Telecommunications. 1: 28–32. (in Russian)

7. Aleksandrov V.V. Pokazateli jeffektivnosti realizacii informacionnyh processov v ITKS v uslovijah protivodejstvija ugrozam informacionnoj bezopasnosti [Indicators of the effectiveness of the implementation of information processes in ITKS in the context of countering threats to information security]. V kn.: Teorija i praktika innovacionnogo razvitija kooperativnogo obrazovanija i nauki [In: Theory and practice of innovative development of cooperative education and science]. Belgorod, Publishing House BUKEP: 18–20.

8. Zaryaev A.V. 2003. Istochniki i kanaly utechki informacii v telekommunikacionnyh sistemah. [Sources and channels of information leakage in telecommunication systems]. Voronezh, Voronezh Institute of the Ministry of Internal Affairs of Russia, 305.

9. Malyuk A.A. 2004. Informacionnaja bezopasnost': konceptual'nye i metodologicheskie osnovy zashhity informacii [Information Security: Conceptual and Methodological Foundations of Information Security]. M., Hotline Telecom, 280.

10. Menshikh V.V. Avsentiev A.O. 2015. A model for optimizing the process of ensuring the requirements for the properties of information during its transmission through communication channels. Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 4: 147–154. (in Russian)

11. Ponomarenko S.V., Ponomarenko S.A., Alexandrov V.V. 2017. Modelirovanie nesankcionirovannogo dostupa k informacionnym resursam kljuchevyh sistem informacionnoj infrastruktury [Modeling of unauthorized access to information resources of key information infrastructure systems]. Belgorod, Publishing House BUKEP, 177.

12. Ponomarenko S.V., Prokushev Ya.E., Alexandrov V.V., Lomazov V.A. 2018. Actual problems of economic security of personal data of information infrastructures of the banking sector. Bulletin of the Belgorod University of Cooperation, Economics and Law. 4: 246–252. (in Russian)

13. Skryl S.V., Mishin D.S. 2005. Ugrozy informacionnoj bezopasnosti v komp'juternyh setjah organov vnutrennih del [Threats to information security in computer networks of internal affairs bodies] In: Sovremennye problemy bor'by s prestupnost'ju [Modern problems of combating crime]. Voronezh, Voronezh Institute of the Ministry of Internal Affairs of Russia, 5–6.

14. Skryl S.V., Spivak V.I., Shcherbakov A.V., Ponomarenko S.V. 2017. The problem of optimization of procedures for integrated technical control of information security against leakage through PEMIN channels: a concept of solution Telecommunications Moscow, Publishing House: Science and Technology LLC, 10: 23–34. (in Russian)

15. Skryl S.V., Finko V.N. Ponomarenko S.V., Volkova S.N., Ryabinin G.I. 2010. Indicator of the effectiveness of information activities of government bodies in the context of countering information leakage through technical channels. Information and Security. 13 (1): 141–142. (in Russian)

16. Khorev A.A. 2008. Tehnicheskaja zashhita informacii: T. 1. Tehnicheskie kanaly utechki informacii. [Technical information security: T. 1. Technical channels of information leakage]. M., NPC "Analytica", 436.

17. Miller D., Harris S., Harper S., VanDyke C. 2010. Security Information and Event Management (SIEM) Implementation. McGraw Hill Professional, 464 p.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Александров Виталий Витальевич, кандидат технических наук, доцент, доцент кафедры организации и технологии защиты информации Белгородского университета кооперации, экономики и права, г. Белгород, Россия

Малий Юлия Васильевна, кандидат экономических наук, доцент кафедры организации и технологии защиты информации Белгородского университета кооперации, экономики и права, г. Белгород, Россия

Александрова Юлия Викторовна, аспирант кафедры организации и технологии защиты информации Белгородского университета кооперации, экономики и права, г. Белгород, Россия

Семенякин Александр Иванович, аспирант кафедры организации и технологии защиты информации Белгородского университета кооперации, экономики и права, г. Белгород, Россия

INFORMATION ABOUT THE AUTHORS

Vitaliy V. Aleksandrov, Candidate of Engineering Science, Associate Professor, Associate Professor of the Department of Organization and Technology of Information Security Belgorod University of Cooperation, Economics and Law, Belgorod, Russia

Yuliya V. Maliy, Candidate of Economic Science, Associate Professor of the Department of Organization and Technology of Information Security Belgorod University of Cooperation, Economics and Law, Belgorod, Russia

Yuliya V. Aleksandrova, Postgraduate student of the Department of Organization and Technology of Information Security Belgorod University of Cooperation, Economics and Law, Belgorod, Russia

Aleksandr I. Semenyakin, Postgraduate student of the Department of Organization and Technology of Information Security Belgorod University of Cooperation, Economics and Law, Belgorod, Russia