Светлана А. Кузьмичёва[1], Олеся В. Тарабрина[2]
[1]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Россия, г. Москва, 115409
e-mail: tz7sveta@yandex.ru, http://orcid.org/0000-0002-3564-1399
[2]Московский государственный технический университет им. Н.Э. Баумана,
2-я Бауманская, 5 стр. 1, Россия, г. Москва, 105005
e-mail: olesya.tarabrina@gmail.com, http://orcid.org/0000-0001-8201-8105

ПОСТРОЕНИЕ АНАЛИТИЧЕСКОЙ СИСТЕМЫ АНАЛИЗА СОБЫТИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

DOI: http://dx.doi.org/10.26583/bit.2019.1.01

Аннотация. В связи с принятием решения о построении государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак организации, имеющие в своем составе критическую информационную инфраструктуру (КИИ), обязаны обеспечить безопасность своих значимых информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, находящихся на территории Российской Федерации. Для предотвращения возможных инцидентов и выполнения требований государства в области защиты КИИ организации должны создать систему безопасности КИИ, обеспечить ее функционирование и подключиться к Национальному координационному центру по компьютерным инцидентам, функционирующему на территории Российской Федерации. В настоящей работе авторами представлен подход к построению аналитической системы для обеспечения информационной безопасности (ИБ) на основе машинного обучения, который позволит оперативно анализировать большие объемы данных о событиях безопасности со всех объектов распределенной вычислительной сети предприятия и принимать взвешенные решения по управлению информационной безопасностью. В ходе исследования выработан перечень основных источников событий информационной безопасности систем и сети, предложена классификация событий для последующего анализа с помощью машинного обучения. Классифицируя события ИБ, полученные из различных систем, а также применяя комплексный подход к оценке ситуации, возможно сделать вывод о состоянии всего объекта защиты в режиме реального времени.
Ключевые слова: аналитическая система, поведенческий анализ, источник событий информационной безопасности, анализ событий, нейронная сеть, машинное обучение.
Для цитирования: КУЗЬМИЧЁВА, Светлана А.; ТАРАБРИНА, Олеся В. ПОСТРОЕНИЕ АНАЛИТИЧЕСКОЙ СИСТЕМЫ АНАЛИЗА СОБЫТИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ. Безопасность информационных технологий, [S.l.], p. 6-14, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1175>. Дата доступа: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.01.

Svetlana A. Kuzmicheva[1], Olesya V. Tarabrina[2]
[1]National Nuclear Research University MEPhI,
Kashirskoye sh., 31, Russia, Moscow, 115409
e-mail: tz7sveta@yandex.ru, http://orcid.org/0000-0002-3564-1399
[2]Bauman Moscow State Technical University,
2nd Baumanskaya, 5bulding1, Moscow, 105005, Russia
e-mail: olesya.tarabrina@gmail.com, http://orcid.org/0000-0001-8201-8105

Building an analytical system for event analysis to ensure information security of the enterprise

DOI: http://dx.doi.org/10.26583/bit.2019.1.01

Abstract. The task of ensuring information security of critical information structures in the Russian Federation is brought to the state level. It requires ensuring the security of information systems, communication networks and technological systems. To prevent possible incidents and meet the requirements of the state the organizations should create a security system for the critical information structures, ensure its functionality, and connect it to National coordination center for computer incidents in order to collect and exchange information about computer attacks. In this paper the authors present an approach to the development of an analytical system for information security based on machine learning, which allow analyzing a large number of events and making informed decisions on information security

management. A list of the main sources of information security events of systems and networks was worked out, and a classification of events for further analysis using machine learning was proposed. By classifying the events obtained from different systems, as well as applying an integrated approach to assessing the situation, it is possible to draw a conclusion about the state of the entire object to be protected in real time.

Keywords: analytical system, user behavior analytics, source of informational security events, analyze of events, machine learning, neural networks.

For citation: KUZMICHEVA, Svetlana A.; TARABRINA, Olesya V. Building an analytical system for event analysis to ensure information security of the enterprise. IT Security (Russia), [S.l.], p. 6-14, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1175>. Date accessed: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.01.

Введение

Информационные технологии заняли важное место в современном мире. Совершенствуются способы поиска, сбора, хранения, обработки, предоставления, распространения информации. С уверенностью можно заявить, что ключевым активом нашей жизни является информация. Однако бурное развитие наблюдается и в способах нелегитимного обращения с информацией, злоумышленники используют всё новые механизмы атак[1,2].

В связи с принятием решения о построении государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак[3,4] задача защиты критической информационной инфраструктуры (КИИ) выводится на государственный уровень.

Закон о КИИ предписывает организациям, к которым относятся органы государственной власти, государственные учреждения и ключевые предприятия основных отраслей экономики Российской Федерации, в которых имеются значимые объекты КИИ, обеспечить безопасность своих информационных систем и информационно-телекоммуникационных сетей, находящихся на территории Российской Федерации. В списке затронутых сфер экономики находится энергетика, в том числе атомная, транспорт, связь, наука, здравоохранение, банковский и финансовый секторы, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленность. Инциденты безопасности на ключевых предприятиях страны могут иметь серьезные последствия в масштабе города, региона и даже целой страны, причин для возникновения инцидентов много: целенаправленные хакерские атаки или случайная ошибка персонала. Для предотвращения возможных инцидентов и выполнения требований государства организации должны создать систему безопасности КИИ, обеспечить ее функционирование и подключиться к системе ГосСОПКА (Государственная система обнаружения предупреждения и ликвидации последствий компьютерных атак) [1].

ГосСОПКА — система предназначенная для сбора и обмена информацией о компьютерных атаках на территории Российской Федерации. Основная цель — предотвращать и противодействовать атакам, в первую очередь внешним, за счет непрерывного мониторинга инцидентов ИБ и своевременной выработки мер противодействия. Для достижения этой цели создается сеть корпоративных и ведомственных центров ГосСОПКА, которая должна охватить все ключевые организации.

---

[1] ФЗ от 27.07.2006 N 149-Федеральный закон «Об информации, информационных технологиях и о защите информации»

[2] О безопасности: Федеральный закон РФ от 28.12.2010 № 390-ФЗ // Собрание законодательства РФ. 03.01.2011. № 1. Ст. 2

[3] ФЗ от 26.07.2017 N 187- Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»

[4] Указ президента Российской Федерации №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

В органах государственной власти строятся ведомственные центры, в государственных корпорациях, операторах связи и лицензиатах в области защиты информации — корпоративные центры. При подключении к ГосСОПКА организации принимают на себя обязательства по незамедлительной отправке сообщений в случае обнаружения компьютерных атак и по реагированию в случае получения информации о возможной атаке [2, 3]. Обнаружив атаку, ведомственный центр ГосСОПКА должен передать информацию в главный центр, который в свою очередь передаст эту информацию другим центрам уже с рекомендациями по противодействию. Такой подход существенно повышает степень готовности и, как следствие, уровень защищенности организаций [4].

Текущий реактивный подход к защите КИИ на данный момент следует стратегии обработки различных событий систем, сети, в том числе анализа журналов логирования информационных систем, проверки использования информации и прав доступа. Однако при неверном реагировании или неверной интерпретации полученных сведений существует возможность получить либо результат false positive (т.е. ложное срабатывание систем защиты), либо стать жертвой успешной атаки.

Наличие централизованной системы обмена информацией о компьютерных инцидентах является преимуществом использования системы ГосСОПКА, однако в зависимости от критичности произошедшего инцидента может требоваться различная скорость реакции, а также крайне желательно наличие оперативной системы реагирования. В связи с этим помимо подключения к упомянутой выше централизованной системе предприятию необходимо проводить аналитику, ориентированную на конкретную инфраструктуру, учитывающую особенности архитектуры организации, установленного программного обеспечения и прохождения информационных потоков.

Особенности конкретной организации необходимо рассматривать при построении аналитической системы в связи со следующими обстоятельствами:

– компоненты инфраструктуры используются аналитической системой в качестве источников событий;

– информационные потоки предприятия используются аналитической системой для определения оптимальных алгоритмов выявления инцидентов информационной безопасности.

Авторами настоящей статьи предлагается подход, позволяющий изменить логику построения защиты КИИ с реактивного на проактивный за счет обеспечения обнаружения аномалий посредством использования алгоритмов машинного обучения [5, 6].

Главная задача аналитической системы – выявление аномальной активности, которая не детектируется классическими средствами защиты, но может свидетельствовать о действиях злоумышленника. Получаемый результат – обнаружение злоумышленника на ранних стадиях атаки.

Работа посвящена классификации источников событий ИБ, а также методам анализа классифицированных событий для определения отклонения от штатного поведения системы. Разработанная аналитическая система позволит оперативно анализировать объемы событий предприятия категории Big data и принимать взвешенные решения по оценке уровня информационной безопасности.

1. Классификация источников событий ИБ

В структурах КИИ, масштаб которых позволяет говорить об использовании средств мониторинга событий ИБ, возможен сбор и классификация событий ИБ посредством аналитической системы.

Под термином «аналитическая система» в рамках данной работы понимается комплекс систем сбора и анализа событий ИБ с возможностью детектирования и классификации определенной угрозы или атаки на основе машинного обучения.

Первоочередной задачей построения аналитической системы является сбор и классификация событий ИБ с целью получения данных для обработки алгоритмами машинного обучения и впоследствии классификации угрозы либо атаки.

Авторами определены методы обработки информации, получаемой из различных источников информации, с помощью которых возможно организовать управление поступающими событиями:

– событие-триггер – реакция системы на одноразовое событие;

– накопительный триггер – реакция системы на повторение одиночного события, может применяться в случаях, когда только повторение события с какой-либо частотой является сигналом для фиксации, наблюдения и реакции;

– статистическая обработка – реакция системы вследствие обнаружения определенной статистики событий ИБ;

– последовательность действий – наиболее сложный классификатор для отслеживания событий. Включает в себя элементы поведенческого анализа пользователя, системы, сети.

Наибольшую сложность для современных решений анализа аномалий составляет количество источников, информация с которых должна быть скоррелирована и проанализирована. Экосистема ИТ-инфраструктуры может быть представлена в соответствии с рис. 1.

Рис. 1. Экосистема ИТ-инфраструктуры
(Fig. 1. IT Infrastructure Ecosystem)

События, необходимые для работы аналитической системы, возможно получать из различных источников, а в дальнейшем классифицировать согласно перечню, представленному ранее.

Авторами настоящей работы предлагается следующий перечень событий ИБ для сбора и анализа:

– Active Directory – информация Logon/Logoff, включение в группы, исключение из групп, выдача определенных прав (например, администратора), создание новых пользователей (групп), активность отключенного аккаунта, активность сервисных аккаунтов, действия администратора, фиксация количества попыток входа;

– сетевое оборудование L2 – события подключения сторонних устройств;

– сетевое оборудование L3 – информация о сетевых взаимодействиях, spoofing-событиях (подмены адреса отправителя), сведения об ошибках на сетевых интерфейсах, объеме трафика, количестве сессий, посещаемых веб-сайтах и внутренних информационных ресурсах, сведения об аутентификации пользователей;

– информация системы класса DLP (Data Leak Prevention) (при наличии системы) – доступ к файлам, события печати (печать большого количества документов, печать определенного типа документов, печать конфиденциальных документов, время печати), email-переписка (письма на определенные домены, письма на свой адрес, письма конкурентам, анализ адреса отправителя, его IP и домена), использование USB и т.д.;

– информация системы класса SIEM (Security information and event management) (при наличии системы) – категорированные данные об активности пользователей и узлов сети, приведенные к единому формату. Уведомления о возможном инциденте ИБ, сгенерированные на основе анализа событий статичными правилами корреляции SIEM;

– Firewall – ftp-коммуникации, загрузка информации на сторонние сайты, контроль количества DNS-запросов, объема DNS-трафика, контроль количества подключений;

– операционная система – получение информации об установленном ПО, запущенных процессах родительском и дочерних.

Для построения аналитической системы перечень источников выработан исходя из доступности, широты охвата эксплуатации систем, оборудования и приложений, которые могут являться источниками событий ИБ. Предложенный авторами перечень источников событий унифицирует перечень обрабатываемых аналитической системой данных, позволяя построить универсальную аналитическую систему с возможностью ее доработки под конкретного потребителя. При этом степень доработки должна уточняться независимо в каждом случае в связи с индивидуальностью ИТ-инфраструктуры каждой организации. Например, производителями систем класса SIEM выделяется более 400 различных источников событий [7], сведения которых могут быть задействованы также в аналитической системе с целью выявления и блокирования атак (рис. 2).

Рис. 2. Интеграция с аналитической системой
(Fig. 2. Integration with analytical system)

Классифицируя события ИБ, полученные из различных систем, применяя комплексный подход к оценке ситуации, возможно, сделать вывод о состоянии всего объекта защиты в режиме реального времени.

2. Анализ событий ИБ

В современных гетерогенных сетях для решения задачи выявления несанкционированного поведения в корпоративной сети эксплуатирующему персоналу необходимо использовать множество решений и достигать результата с применением их совокупности.

Наличие большого количества независимых решений делает невозможной корреляцию цепи событий и выявления направленных атак и аномалий. Для централизации механизма принятия решений об обнаружении аномалий необходимо аккумулировать перечень методов, на основании которых может быть принято решение об аномалии, основанное на большом количестве источников информации, так как различные виды аномалий могут быть зафиксированы различными алгоритмами.

При работе с данными большого количества современных систем аналитическая система будет базироваться в своих решениях на сведениях, полученных в результате обучения. В рамках обучения производится наблюдение за актуальными процессами как при взаимодействии между информационными системами, так и в рамках каждой отдельной системы.

Таблица 1. Перечень методов для выявления аномалий

Наименование	Принцип действия	Пример
Триггер	Наступление определенного события классифицируется как инцидент	Пользователь обратился к ресурсу, доступ к которому ему запрещен
Накопительный триггер	Повторение какого-либо одного события количество раз, превышающее пороговое, классифицируется как инцидент	Пользователь произвел более 100 неуспешных попыток аутентификации при попытке доступа к ресурсу
Статистический анализ	Повторение группы событий количество раз, превышающее пороговое, классифицируется как инцидент	Пользователь обратился к ресурсу, к которому ранее не обращался
Экспертная система	Наступление события, зафиксированного в базе знаний, классифицируется как инцидент	Пользователь направляет в БД нетиповые запросы, содержащие признаки попыток компрометации данных
Машинное обучение	Отклонение от состояния, изученного системой, на заданное пороговое значение, классифицируется как инцидент	Пользователь за рабочий день выполнял неоднократную отправку писем с зашифрованными вложениями на некорпоративные рабочие ящики и копировал большие объемы данных на внешний накопитель, хотя подобный вид деятельности не входит в его типовые должностные обязанности

Единой классификации методов обнаружения аномалий не существует. Наряду с предлагаемыми классификациями методов обнаружения аномалий, включающими в себя разделение на поведенческие методы, методы машинного обучения и методы вычислительного интеллекта [8], учет возможности многошаговой корреляции [14], конечные автоматы, правилоориентированный метод, рассуждение на основе прецедентов, байесовская сеть, нейронная сеть [15], выделяют также методы обнаружения злоупотреблений, включающие в себя помимо методов машинного обучения и методов вычислительного интеллекта методы на основе знаний [16].

Авторами статьи предлагается перечень методов, которые могут быть использованы для выявления аномалий, представленный в таблице 1.

Стоит отметить, что помимо формирования перечня методов выявления аномалий, которые используются аналитической системой, также прорабатываются подходы к использованию методов для выявления атак, например: построение системы интеллектуальных сервисов защиты информации [9] с учетом особенностей критически важных инфраструктур [10], генерация модели атак [11], анализ в соответствии с уровнями модели ISO/OSI [12], оптимизация архитектуры системы под задачи работы с большими массивами данных и учет возможности масштабируемости [13] и другие.

Предлагаемый перечень методов, закладываемый в основу аналитической системы, определен на основании наиболее широко распространенных методов. Разрабатываемая аналитическая система должна поддерживать работу со всеми перечисленными методами, а также обладать возможностью автоматического выбора наиболее оптимального метода для определения различных видов аномалий. Предложенный авторами перечень методов позволит определить аномалии на основании сформулированного перечня источников.

Стоит отметить, что сформированные авторами перечни источников событий и методов актуальны не только для КИИ, но и для корпоративной сети иных предприятий.

Заключение

Инициирование построения государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак поставило вопрос о разработке организациями, имеющими в своем составе КИИ, собственных аналитических систем для централизованного сбора и обработки сведений о состоянии информационной безопасности КИИ собственного предприятия.

Авторами статьи сформулирован и представлен перечень источников событий, информацию о которых необходимо направлять для анализа в аналитическую систему. Эти события могут использоваться системой для принятия решения о наличии инцидента на защищаемом ресурсе.

Также авторами представлен перечень методов, который может использоваться аналитической системой для анализа поступающих событий, их корреляции и принятия решения о наличии в поступивших событиях свойств инцидента информационной безопасности.

Направлением дальнейших исследований является изучение параметров событий для обработки алгоритмами машинного обучения, построение моделей прохождения процесса обработки событий, выбор, разработка и реализация алгоритмов.

СПИСОК ЛИТЕРАТУРЫ:

1. Марков А.С. Технические решения по реализации подсистем ГосСОПКА // Материалы конференции «Управление информационной безопасностью в современном обществе», Москва, 30 мая – 1 июня, 2017. С. 85 – 96.
2. Ежгуров В.Н., Юмашева Е.С., Бач М.А. Проблемы внедрения системы обнаружения вторжения и устранения компьютерных атак // Материалы конференции ГНИИ «Нацразвитие», Санкт-Петербург, январь, 2018. С. 19 – 27.
3. Сироткин Д.В., Рекунков И.С., Лазунин К.А., Ильин К.В. Технические аспекты создания системы защиты информационного пространства // Информационные войны. 2017. № 3 (43). С. 84 – 88.

4. Столяров В. Безопасность критической информационной инфраструктуры как она есть // Системный администратор. 2018. № 1-2 (182-183). С. 10 – 14.
5. Бринк Х., Ричардс Д., Феверолф М. Машинное обучение. СПб.: «Питер», 2017. 336 с.
6. Хайкин С. Нейронные сети: полный курс. 2-е изд. М., «Вильямс», 2006. 1104 с.
7. Самсонова В.Г., Кулинич Р.С. Сравнительный анализ систем управления информационной безопасностью и событиями безопасности // Безопасные информационные технологии. Сборник трудов Седьмой всероссийской научно-технической конференции / под. ред. В.А. Матвеева – М.: МГТУ им. Н.Э.Баумана, 2016. С. 248 – 253.
8. Кожевникова И. С. Анализ методов обнаружения аномалий для обнаружения сканирования портов // Молодой ученый. – 2017. – № 14. – С. 31 – 34. URL https://moluch.ru/archive/148/41829/ (дата обращения: 12.07.2018)
9. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. Вып. 3(22). С. 84 – 100.
10. Котенко И.В., Саенко И.Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. Вып. 1(24). С. 21 – 40.
11. Дойникова Е.В., Котенко И.В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер // Труды СПИИРАН. 2018. № 2 (57). С. 211 – 240.
12. Василишин Н.С., Ушаков И.А, Котенко И.В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // Аллея науки. 2018. № 6(22). С. 1012 – 1021.
13. Котенко И.В., Кулешов А.А., Ушаков И.А. Система сбора, хранения и обработки информации и событий безопасности на основе средств elastic stack // Труды СПИИРАН. 2017. № 5 (54). С. 5 – 34.
14. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в siem-системах. Часть 1 // Труды СПИИРАН. 2016. № 4 (47). С. 5 – 27.
15. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в siem-системах. Часть 2 // Труды СПИИРАН. 2016. № 6 (49). С. 208 – 225.
16. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2 (45). С. 207 – 244.

REFERENCES:

[1] Markov A.S. Technical solutions for the implementation of subsystems of GosSOPKA. Materialy konferencii «Upravlenie informacionnoj bezopasnost'ju v sovremennom obshhestve», Moskva, 30.05 – 01.05.2017. P. 85 – 96. (in Russian).
[2] Ezhgurov V.N., Jumasheva E.S., Bach M.A. Problems of introducing an intrusion detection system and eliminating computer attacks. Materialy konferencii GNII «Nacrazvitie», Sankt-Peterburg, January, 2018. P. 19 – 27. (In Russian).
[3] Sirotkin D.V., Rekunkov I.S., Lazunin K.A., Il'in K.V. Technical aspects of creating a system for protecting the information space. Informacionnye vojny. 2017. № 3 (43). P. 84 – 88. (in Russian).
[4] Stoljarov V. Security of critical information infrastructure as it is. Sistemnyj administrator. 2018. № 1-2 (182-183). P. 10 – 14. (in Russian).
[5] Brink H., Richards D., Feverolf M. Real-World Machine Learning Spb «Piter», 2017. 336 p. (in Russian).
[6] Haykin S. Neural Networks: A Comprehensive Foundation. 2-e izd. M., «Vil'jams», 2006. 1104 p. (in Russian).
[7] Kozhevnikova I. S. Analysis of detecting anomalies methods for detecting port scans.Molodoj uchenyj. – 2017. – №14. – P. 31 – 34. URL https://moluch.ru/archive/148/41829/ (data accessed: 12.07.2018). (in Russian).
[8] Samsonova V.G., Kulinich R.S. Comparative analysis of the security information and event management systems. Bezopasnyye informatsionnyye tekhnologii. Sbornik trudov Sed'moy vserossiyskoy nauchno-tekhnicheskoy konferentsii / pod. red. V.A. Matveyeva – M.: MGTU im. N.E.Baumana, 2016. P. 248 – 253. (in Russian).
[9] Kotenko I.V., Saenko I.B. Developing the system of intelligent services to protect information in cyber warfare. Trudy SPIIRAN. 2012. V. 3(22). P. 84 – 100. (in Russian).
[10] Kotenko I.V., Saenko I.B. Architecture of the system of intelligent information security services in critical infrastructures. Trudy SPIIRAN. 2013. V. 1(24). P. 21 – 40. (in Russian).
[11] Dojnikova E.V., Kotenko I.V. Improvement of attack graphs for cybersecurity monitoring: handling of inaccuracies, processing of cycles, mapping of incidents and automatic countermeasure selection. Trudy SPIIRAN. 2018. № 2 (57). P. 211 – 240. (in Russian).
[12] Vasilishin N.S., Ushakov I.A, Kotenko I.V. Network traffic analysis algorithms based on BigData technologies used for network attacks detection. Alleya nauki. 2018. № 6(22). P. 1012 – 1021. (in Russian).
[13] Kotenko I.V., Kuleshov A.A., Ushakov I.A. A system for collecting, storing and processing security information and events based on elastic stack tools. Trudy SPIIRAN. 2017. № 5 (54). P. 5 – 34. (in Russian).
[14] Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. An Analysis of Security Event Correlation Techniques in Siem-Systems. Part 1. Trudy SPIIRAN. 2016. № 4 (47). P. 5 – 27. (in Russian).

[15] Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. An Analysis of Security Event Correlation Techniques in Siem-Systems. Part 2. Trudy SPIIRAN. 2016. № 6 (49). P. 208 – 225. (in Russian).
[16] Branickij A.A., Kotenko I.V. Analysis and Classification of Methods for Network Attack Detection. Trudy SPIIRAN. 2016. № 2 (45). P. 207 – 244. (in Russian).

Поступила в редакцию - 26 декабря 2018 г. Окончательный вариант – 30 января 2019 г.
Received – December 26, 2018. The final version – January 30, 2019.