ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI:10.21822/2073-6185-2022-49-4-78-84 Обзорная статья/ Review article

Анализ технологий защиты информации для использования в инфраструктуре предприятия

А.Д. Попов, А.Д. Попова
Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия,

Резюме. Цель. Целью исследования является анализ современных технологий информационной безопасности для решения задач защиты информации инфраструктуры предприятия. **Метод.** Исследование основано на методах системного анализа, синтеза, дедукции. **Результат.** Проведен анализ и раскрыты особенности технологии защиты информации с целью возможного использования в инфраструктуре предприятия. Проведен анализ отечественного и зарубежного программного обеспечения для практического использования. **Вывод.** Результаты проведенного анализа раскрывают особенности использования средств защиты информации в инфраструктуре предприятия в целях противодействия современным векторам атак на информационные ресурсы.

Ключевые слова: программные средства, информационная безопасность, системы защиты информации

Для цитирования: А.Д. Попов, А.Д. Попова. Анализ технологий защиты информации для использования в инфраструктуре предприятия. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(4):78-84. DOI:10.21822/2073-6185-2022-49-4-78-84

Analysis of information security technologies for use in the enterprise infrastructure

A.D. Popov, A.D. Popova
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov Ave., Voronezh 394065, Russia

Abstract. Objective. The purpose of the study is to analyze modern information security technologies for solving the problems of protecting information in the enterprise infrastructure. **Method.** The study is based on the methods of system analysis, synthesis, deduction. **Result.** The analysis was carried out and the features of information protection technology were disclosed for the purpose of possible use in the infrastructure of the enterprise. The analysis of domestic and foreign software for practical use is carried out. **Conclusion**. The results of the analysis reveal the features of using information protection tools in the enterprise infrastructure in order to counteract modern vectors of attacks on information resources.

Keywords: software, information security, information security systems

For citation: A.D. Popov, A.D. Popova. Analysis of information security technologies for use in the enterprise infrastructure. Herald of Daghestan State Technical University. Technical Science. 2022; 49(4):78-84. DOI:10.21822/2073-6185-2022-49-4-78-84

Введение. Современный мир, любая сфера деятельности человека характеризуется использованием различных служб и сервисов, обеспечивающих работу производственных систем. В связи с этим нарушение их нормальной работы могут быть связаны с техническими неполадками, неквалифицированными действиями персонала, преднамеренными злонамеренными действиями и т.д. Все это может привести к потере денежных средств, компрометации документов, нарушению штатного функционирования систем и т.д., что естественным образом может при-

вести к различным негативным последствиям. Следует отметить, что инфраструктура и технологический стек предприятий, государственных учреждений, частных компаний зависит в основном от стоящих перед ними задач, что требует фактически индивидуальных подходов к разработке эксплуатационных регламентов, разработке нормативных актов, выбора организационных мер защиты информации и т.д. Развитие подобных служб, сервисов и в целом информационных технологий в настоящее время осуществляется колоссальными темпами. В связи с этим происходит углубленная декомпозиция задач, которые должны осуществляться программным обеспечением. Данный подход используется при разработке высоконагруженных, критичных и распределенных систем.

Постановка задачи. На практике сложность проектирования и эксплуатации подобных систем вызвана трудностью конфигурирования, контроля правильности разработки программного обеспечения, выделения ресурсов, сбора метрик, подготовленностью персонала и т.д. Также немаловажным фактором являются условия эксплуатации, а именно выбор в пользу облачных ресурсов или же физического сервера. С учетом того, что подобных программных продуктов может быть ни один десяток, масштаб всех неопределенностей может привести к кризисной ситуации. При решении подобных задач могут быть преднамеренно упущены множество нюансов, которые с одной стороны облегчат разработку, внедрение и эксплуатацию, но с другой стороны задачи и цели, стоящие перед персоналом, могут быть достигнуты не в полной мере. Зачастую подобные упущения влекут за собой нарушения информационной безопасности, некорректную работу программного обеспечения, появление уязвимых мест и т.д.

Меры защиты в организации применяются в соответствии с критичностью обрабатываемой информации. Также немаловажным фактором при их выборе является структура организации, используемые технические и программные средства и др. В целом все подходы к защите информации определяются политикой информационной безопасности.

В связи с увеличением количества компьютерных атак и появлением новых векторов их реализации встает острый вопрос выявления, анализа и хранения информации по ним. Для решения данной задачи поверх всех традиционных средств защиты информации внедряются программные средства автоматизации обнаружения угроз и реагирование на них. В настоящее время для решения задач информационной безопасности в автоматизированные системы различного уровня сложности внедряются средства защиты информации. Данные средства можно разделить на два больших класса одни представляют уже готовое техническое устройство, другие реализованы в программном исполнении.

Программные средства можно разделить на локальные(антивирусы, системы защиты информации от несанкционированного доступа и др.) устанавливаемые на автоматизированное рабочее место и распределенные(Extended Detection and Response (XDR), Security information and event management (SIEM), Security Orchestration, Automation and Response (SOAR) и др.) устанавливаемые на сервер и имеющие агентов исполнителей. Естественно, что данные программные средства выполняют различные задачи, но все же объединены одной главной целью «Защита информации». Локальные, представлены широким классом инструментов защиты информации. Мировому сообществу известны множество методологических работ, нормативных актов, регламентирующих их работу [1-3]. Средства защиты информации в распределенном исполнении также имеют множество научных работ, но нормативных актов, регламентирующих их работу, практически нет [4,5]. Это обусловлено тем что законодатель не успевает за технологическим прогрессом, а тем более рассмотреть каждую инфраструктуру в определенной конфигурации отдельно. Также специалист, принимающий архитектурные решения в организации, не может сразу определить какие распределенные решения по защите информации необходимы, будут ли они избыточными, нужно вообще их внедрять и т.д. В связи с этим задача статьи заключается в анализе технологий и программных средств их реализующих, позволяющих распределённой(комплексно) защитить организацию от современных компьютерных атак и угроз информационной безопасности.

Методы исследования. Сложность и многовекторность компьютерных атак повлияла на развитие программных продуктов для их противодействия. Данный факт говорит о все большей неопределенности при выборе программных продуктов. Наиболее распространенный классом рассматриваемых систем являются SIEM [6, 7]. Данные системы предназначены для мониторинга, сбора и обработки различных событий информационной безопасности. Принцип функционирования SIEM систем заключается в том, что данные о безопасности информационных систем собираются в реальном времени из различных источников и по результатам их обработки предоставляются отчеты в едином интерфейсе. Полученные сведения предоставляются аналитику безопасности, и в последующем исследуются на наличие характерных особенностей, соответствующих инцидентам информационной безопасности. SIEM обеспечивает защиту от различного рода атак, а также имеет следующие возможности, представленные на рис. 1.

SIEM системы довольно быстро завоевывают рынок средств защиты информации и представляют собой технологический гибрид по сбору информации со всевозможных источников, начиная с сетевых устройств заканчивая контейнерами. Анализ архитектур современных SIEM систем показал, что разработчики опираются на различные технологические концепции и решения (на основе виртуальных машин, на основе микросервисной архитектуры, предоставляют программное обеспечение как сервис в облачной инфраструктуре), что дает большую гибкость в выборе того или иного решения. Более подробно архитектурные решения типовых SIEM систем будут рассмотрены в последующих статьях.

Рис. 1 Функциональные возможности SIEM систем
Fig. 1. Functionality of SIEM systems

Обсуждение результатов. При внедрении в организации подобных систем возникает ряд трудностей, связанных с обучением сотрудника, отвечающего за контроль и эксплуатацию подобной системы. Зачастую у организации встает выбор эксплуатировать SIEM систему на собственных ресурсах, либо на облачных (преимущественно используются большими организациями), или же отдать полное право контроля в аутсорсинговую компанию, которая функционирует в рамках Security Operation Center (SOC) центр обеспечения компьютерной безопасности. В случае если выбор падает в пользу аутсорсинговой компании, то значительная часть защитных функций будет в руках сторонней организации, что с одной стороны снимает проблему с вводом в штат нового сотрудника, но в тоже время увеличивает риски утечки информации. Каждая из стратегий имеет свои плюсы и минусы, которые следует учитывать. На мировом рынке SIEM систем представлены следующие программные решения IBM QRadar SIEM, McAfee Enterprise Security Manager, Micro Focus ArcSight 2021.1, FortiSIEM (Fortinet). На отечественном рынке представлено множество SIEM систем, к ним можно отнести: MaxPatrol, RuSIEM, KOMRAD Enterprise SIEM, Kaspersky Unified Monitoring and Analysis Platform и др. Данные решения представляет широкий спектр программных компонентов, позволяющих выявлять отклонения от нормальной работы системы и др. Представленные системы активным образом развиваются, добавляя в продукты новые технологические решения. SIEM системы положили начало технологиям поведенческого анализа пользователей User and entity behavior

analytics (UEBA), оркестрации безопасности и автоматического реагирования Security orchestration and automation response (SOAR).

Первая основывается на искусственном интеллекте и методах глубокого обучения для изучения моделей человеческого поведения. UEBA обнаруживает угрозы, определяя действия пользователя или систем, которые отклоняются от нормы. Чаще всего используется для отслеживания и обнаружения подозрительного трафика, несанкционированного доступа к данным, а также вредоносной активности в компьютерной сети или на ее узлах. Данная технология помогает выявить целевые атаки, попытки мошенничества, внутренних нарушителей. UEBA применяет аналитические методы для анализа данных, характеризующих поведение пользователя и событий, возникающих в операционной системе [8,9]. Полученные данные сравниваются с базовым поведением, что позволяет обнаружить аномалии, а также провести оценку риска и определить, допустимы ли отклонения. Если оценка превышает пороговый уровень, то система оповещает аналитиков безопасности. Данная технология активно интегрируется в SIEM, но все же представляет собой отдельный инструмент. К самым распространенным можно отнести Fortinet, Gurucul UEBA, Splunk, Cynet, LogRhythm, Rapid7, Exabeam.

SOAR представляют собой набор программных решений и инструментов, предназначенных для просмотра и сбора данных различной природы [10,11]. Это позволяет провести подробный анализ на основе человеческого и машинного обучения с целью определения приоритетов для действий по реагированию на инциденты. Человеческим фактором является проведение машинного обучения, объяснение полученных результатов в особенности, когда они противоречат здравому смыслу. SOAR решает три основные задачи: управление угрозами и уязвимостями, автоматизация операций реагирования на инциденты безопасности. Это достигается путем сбора данных об угрозах из различных источников и автоматизированного реагирование на них.

По итогам анализа были выявлены следующие программные решения: Swimlane SOAR, Splunk Phantom, Security Vision IRP/SOAR, Cortex XSOAR, Siemplify, FortiSOAR, RVision IRP и Eplat4m SOAR. Если разница между SIEM и UEBA очевидна, то с SOAR нет. SOAR системы стремятся уменьшить количество задач, стоящих перед аналитиком безопасности (путем интеллектуального управления угроза и уязвимостями) и автоматизировать их, а также объединить все возможные решения информационной безопасности с целью недопущения ложных срабатываний. В отличие от SIEM SOAR является более продвинутым технологическим решением, которое позволяет получать события из классических инструментов информационной безопасности, а также более быстро проводить судебную экспертизу и т.д. (рис. 2), где IDS/IPS (Intrusion Detection System/ Intrusion Prevention System) – системы обнаружения и предотвращения вторжений.

Рис. 2. Функциональные особенности SOAR систем
Fig. 2. Functional features of SOAR systems

Существует еще один класс технологических решений таких, как Endpoint detection and response (EDR) [12,13]. Данные системы призваны предупреждать аналитиков безопасности о злонамеренной активности, а также обеспечивать быстрое расследование и сдерживание атак на конечные точки. При помощи агентов с устройств собирается информация о выполнении про-

цессов, журналах событий, запущенных приложениях, сетевой активности, аутентификации пользователей в системе с последующим ее корреляцией и анализом. EDR позволяют выполнять автоматические и ручные действия по сдерживанию, например, автоматически останавливать скомпрометированные процессы, изолировать и отключать подозрительные учетные записи и устройства. Зачастую EDR интегрируются с SIEM системами. На рынке представлены следующие инструменты Kaspersky Endpoint Detection and Response Expert, Symantec Endpoint Protection, RSA NetWitness Endpoint, CrowdStrike Falcon Insight, Cybereason Endpoint Detection and Response, FireEye Endpoint Security. Развитием EDR стали системы класса XDR [14].

Вторые в отличие от первых осуществляют активный поиск угроз, которые не могут быть выявлены обычными средствами защиты информации, такими как брандмауэры или системами антивирусного мониторинга. Это достигается введением дополнительных сканеров на сетевые узлы, сканеров поведенческого анализа, инструментов обобщения данных сети, устройств и др. В системах XDR сбор событий осуществляется не только на устройствах, но, а также на сетевых сенсорах, межсетевых экранах, шлюзах безопасности, облачных серверах, IDS/IPS, SIEM и др. Обобщенно основами задачами подобных систем является комплексное обнаружение угроз, аналитика, реагирование и расследование атак.

Представленные технологии схожи между собой, но в классическом составе они содержат меньше функций чем XDR, а именно:

- EDR обеспечивают защиту информации на уровне устройств без возможности контроля сетевых и облачных служб.
- SIEM собирают и анализируют информации в локальной сети без возможности реагирования.
- UEBA проводят поведенческий анализ пользователей, приложений и устройств без возможности реагирования на аномалии.
- SOAR работают в основном по сигнатурам и типовым сценариям реагирования и охватывают большую часть инфраструктуры, но не обеспечивая проактивную защиту.

Перспективной классом средств защиты информации является Cybersecurity Mesh Architecture (CSMA) технология комплексной безопасности, которая представляет собой выделенный уровень инфраструктуры для облегчения взаимодействий между всеми возможными средствами защиты информации, что позволяет противостоять всем видам атак [15]. Основной идеей организации работы CSMA систем является политика нулевого доверия. Она применяет индивидуальные подходы к аутентификации на всех функционирующих устройствах и используемых ресурсах (не доверяет по умолчанию).

Подобная практика устраняет пробелы классической политики безопасности, ориентированной на контроль устройств в локальной сети, а также позволяет обнаруживать и устранять угрозы на ранней стадии. Системами типа CSMA выделяются четыре вспомогательных уровня, каждый из которых имеет свою зону ответственности. Главная задача которых, обеспечить взаимодействие всех технологий защиты информации (рис. 3).

Аналитика безопасности. Данный уровень направлен на сбор, агрегацию и анализ данных о безопасности из различных источников. На их основе SIEM и SOAR идентифицируют потенциальные угрозы и осуществляют противодействие.

Распределенная регистрация. Уровень ориентирован на предоставление службам управления идентификацией возможности децентрализованного контроля над каталогами, аутентификацией пользователей, правами доступа, что и определяет политику безопасности с нулевым доверием.

Консолидированное управление политиками и состоянием. Данный уровень осуществляет миграцию политик безопасности из различных сред, с целью согласованного управления всеми частями системы. А именно, происходит преобразование правил и параметров конфигурации конкретной среды для динамической авторизации при использования другой.

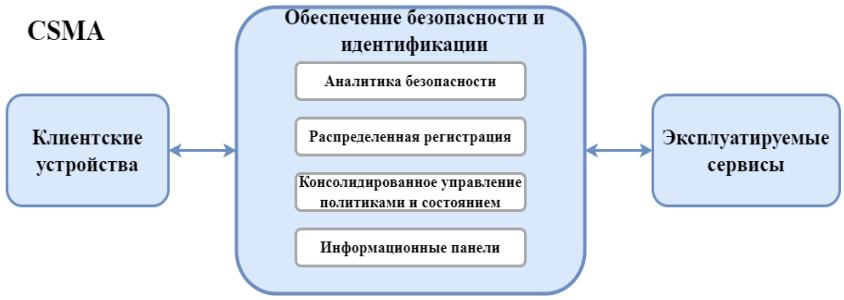

Рис.3. Уровни взаимодействия CSMA с инструментами защиты информации
Fig.3. Levels of interaction between CSMA and information security tools

Информационные панели. Этот уровень обеспечивает возможность контроля всей архитектуры безопасности, позволяя более эффективно обнаруживать, исследовать и реагировать на инциденты безопасности. Это достигается путем переключения между несколькими информационными панелями, либо за счет обобщения информации из различных источников в одной панели.

Вывод. Анализ рынка CSMA систем показал, что готовых решений, предоставляющих подобную функциональность нет. В перспективе возможность реализации данной технологии просматривается у Лаборатории Касперского. Результаты анализа показали, что мировое сообщество готово к противодействию современным векторам атак. Но в тоже время у конечного пользователя (администратора безопасности) остается множество вопросов, связанных с необходимостью использования подобных систем, в частности полноты функциональных компонентов, стоимости, поддержки и т.д. Естественным фактором выбора подобных систем будет является задачи, стоящие перед организацией, уровень обрабатываемой информации, количество пользователей и др. У каждого производителя существует свой набор функциональных компонентов, используются гибридные варианты, заимствуются элементы другого класса систем, что с одной стороны позволит предостеречь от большего количества атак, но с другой может быть избыточным. Это в очередной раз подтверждает важность оценки риска и глубокого понимания угроз безопасности к информационным системам определенного типа. Представленная работа раскрывает основные особенности функционирования средств защиты информации для инфраструктуры предприятия, что позволяет сделать выбор в пользу той или иной технологии исходя из потребностей.

Библиографический список:

1. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Эл. ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (дата обращения 20.06.2022).
2. ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации [Электронный ресурс]. — URL:http://fstec.ru/component/attachment s/ 299 (дата обращения: 26.06.2022).
3. Гостехкомиссия РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М.: Воениздат, 1992. – 29 с.
4. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2012. № 20 (1). С. 27-56.
5. Gustavo González-Granadillo ,Susana González-Zarzosa and Rodrigo Diaz Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures Sensors 2021, 21(14), 4759.
6. 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. № 47 (4). С. 5-27.
7. 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. № 49 (6). С. 208-225.
8. Котенко И.В., Ушаков И.А., Пелёвин Д.В., Преображенский А.И., Овраменко А.Ю. Выявление инсайдеров в корпоративной сети: подход на базе UBA и UEBA // Защита информации. Инсайд. 2019. № 5 (89). С. 26-35.
9. Федоров В.А., Щипцов Д.И. Обзор методов обнаружения инсайдеров в компьютерных сетях с применением UEBA-систем // European science forum. сборник статей IV Международной научно-практической конференции. Петрозаводск, 2020. С. 50-53.

10. Богданов В.В., Домуховский Н.А., Савин М.В. SOAR: автоматизация работы с инцидентами информационной безопасности // Защита информации. Инсайд. 2021. № 3 (99). С. 13-17.
11. Селезнёв В.М., Боровская О.Е. Встраивание инструментов SOAR-платформ в экосистему SOC для автоматизации процесса реагирования на инциденты ИБ // Международный научно-исследовательский журнал. 2022. № 10 (124).
12. Васильева И.Н. Современный подход к мониторингу безопасности сетевых информационных инфраструктур // Инновационные технологии и вопросы обеспечения безопасности реальной экономики. сборник научных трудов по итогам III Всероссийской научно-практической конференции. Санкт-Петербург, 2021. С. 24-32.
13. Безпалов М.Ю., Ланец С.А. Современные вызовы и технологические решения информационной безопасности // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке. 2022. Т. 1. С. 181-186.
14. Савин М.В., Стойчин К.Л., Некрасов А.В., Комаров Н.В. Обзор стандартов и форматов представления автоматизированных сценариев реагирования на инциденты компьютерной безопасности // Защита информации. Инсайд. 2022. № 4 (106). С. 14-19.
15. Sneps-Sneppe M., Namiot D. Rethinking the power of packet switching in the coming cyber threats era International Journal of Open Information Technologies. 2019. Т. 7. № 8. С. 48-58.

References:

1. FSTEC RF. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and requirements for information protection [El.res.]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (Date of circulation 06/20/2022). (In Russ)
2. FSTEC RF. Guidance document. The concept of protection of computer equipment and automated systems from unauthorized access to information [El. Res.]. URL: http://fstec.ru/component/attachment s/ 299 (date of access: 06/26/2022). (In Russ)
3. State Technical Commission of the Russian Federation. Guidance document. Computer facilities. Protection against unauthorized access to information. Indicators of security from unauthorized access to information. M.: Military Publishing House, 1992; 29. (In Russ)
4. Kotenko I.V., Saenko I.B., Polubelova O.V., Chechulin A.A. Application of Information and Security Events Management Technology for Information Protection in Critical Infrastructures. *Proceedings of SPIIRAS*. 2012; 20 (1): 27-56. (In Russ)
5. Gustavo González-Granadillo , Susana González-Zarzosa and Rodrigo Diaz Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures Sensors 2021; 21(14): 4759.
6. Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. Analysis of security event correlation methods in SIEM systems. Part 1. *Proceedings of SPIIRAS*. 2016; 47 (4): 5-27. (In Russ)
7. Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. Analysis of security event correlation methods in SIEM systems. Part 2 . *Proceedings of SPIIRAS*. 2016; 49 (6):208-225. (In Russ)
8. Kotenko I.V., Ushakov I.A., Pelevin D.V., Preobrazhensky A.I., Ovramenko A.Yu. Identification of insiders in a corporate network: an approach based on UBA and UEBA. *Information Security. Inside.* 2019; 5 (89): 26-35. (In Russ)
9. Fedorov V.A., Shchiptsov D.I. Overview of insider detection methods in computer networks using UEBA systems. European science forum. Collection of articles of the IV International scientific-practical conference. Petrozavodsk, 2020; 50-53. (In Russ)
10. Bogdanov V.V., Domukhovsky N.A., Savin M.V. SOAR: automation of work with information security incidents. *Information security. Inside*. 2021; 3 (99): 13-17. (In Russ)
11. Seleznev V.M., Borovskaya O.E. Embedding SOAR platform tools in the SOC ecosystem to automate the process of responding to information security incidents. *International Research Journal.* 2022; 10 (124). (In Russ)
12. Vasilyeva I.N. A modern approach to monitoring the security of network information infrastructures. Innovatsionnye tekhnologii i voprosy obespecheniya bezopasnosti real ekonomiki. Collection of scientific papers based on the results of the III All-Russian scientific and practical conference. St. Petersburg, 2021; 24-32. (In Russ)
13. Bezpalov M.Yu., Lanets S.A. Modern challenges and technological solutions for information security. Scientific, technical and economic cooperation of the Asia-Pacific countries in the XXI century. 2022; 1: 181-186. (In Russ)
14. Savin M.V., Stoichin K.L., Nekrasov A.V., Komarov N.V. Overview of standards and formats for the presentation of automated scenarios for responding to computer security incidents. *Information Security. Inside*. 2022; 4 (106): 14-19. (In Russ)
15. Sneps-Sneppe M., Namiot D. *Rethinking the power of packet switching in the coming cyber threats era International Journal of Open Information Technologies.* 2019;7(8): 48-58.

Сведения об авторах:

Попов Антон Дмитриевич, кандидат технических наук, старший преподаватель кафедры автоматизированных информационных систем органов внутренних дел; anton.holmes@mail.ru

Попова Арина Дмитриевна, слушатель; arnpva@mail.ru

Information about the authors:

Anton D. Popov, Cand. Sci. (Eng.), Senior Lecturer of the Department of Automated Information Systems of Internal Affairs Bodies; anton.holmes@mail.ru

Arina D. Popova, Student; arnpva@mail.ru

Конфликт интересов/ Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 04.11.2022.

Одобрена после/рецензирования Reviced 27.11.2022.

Принята в печать/ Accepted for publication 27.11.2022.