УДК 004.056.5

***С. П. Киргизбаев [1], В. П. Киргизбаев [1], А. А. Бутин [1]***

*[1] Иркутский государственный университет путей сообщения, г. Иркутск, Россия*

# ПРИМЕНЕНИЕ РЕШЕНИЙ ATTACK SURFACE MANAGEMENT ДЛЯ АВТОМАТИЗАЦИИ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНОЙ СЕТИ

***Аннотация.*** В данной статье рассматривается актуальная проблема XXI века – быстро расширяющаяся поверхность атаки организаций, происходящая вследствие усиления цифровизации бизнес-процессов. Показан один из самых эффективных способов решения данной проблемы – применение продуктов для управления поверхностью атаки компании. Особое внимание уделяется существующим на международном и отечественном рынках продуктам Attack Surface Management. В работе подробно исследованы такие зарубежные продукты, как Randori (IBM), Mandiant (Google), Cortex Xpanse (Palo Alto Networks), отечественный продукт Attack Surface Management (F.A.C.C.T., ранее – Group-IB). Так же в данной статье сравниваются между собой отечественные и зарубежные решения по различным ключевым критериям.

***Ключевые слова:*** информационная безопасность, мониторинг, аудит, сканирование уязвимостей, управление поверхностью атаки, информационные активы, облачные технологии.

***S. P. Kirgizbaev [1], V. P. Kirgizbaev [1], A. A. Butin [1]***

*[1] Irkutsk State Transport University, Irkutsk, Russian Federation*

# APPLICATION OF ATTACK SURFACE MANAGEMENT SOLUTIONS FOR AUTOMATION OF INFORMATION SECURITY MONITORING IN THE CORPORATE NETWORK

***Abstract.*** This article discusses an urgent problem of the XXI century – the rapidly expanding attack surface of organizations, which occurs due to the increased digitalization of business processes. One of the most effective ways to solve this problem is shown – the use of products to control the attack surface of the company. Special attention is paid to the Attack Surface Management products existing on the international and domestic markets. In the work, such foreign products as Randori (IBM), Mandiant (Google), Cortex Xpanse (Palo Alto Networks), the domestic product Attack Surface Management (F.A.C.C.T., formerly Group–IB) are studied in detail. Also in this article, domestic and foreign solutions are compared with each other according to various key criteria.

***Keywords:*** information security, monitoring, audit, vulnerability scanning, attack surface management, information assets, cloud technologies.

## Введение

Массовое внедрение цифровых и облачных технологий для оптимизации бизнес-процессов, быстрое расширение пространства общедоступных IP-адресов не позволяют организациям своевременно определять изменение поверхности атаки. Поверхность атаки организации – это совокупность всех потенциальных маршрутов, которые злоумышленник может использовать в качестве точки первоначального проникновения [1]. Например, поверхность атаки может состоять из веб-формы входа в систему, доступной злоумышленнику для взлома методом грубой силы; из неправильно сконфигурированного облачного хранилища, открытого для общего доступа; из неисправленного Java-приложения [2], работающего на сервере, который, как считает компания, был выведен из эксплуатации много лет назад; или даже из системы в цепочке поставок подрядчика организации (такой как система выставления счетов и учёта), имеющей доступ к сети компании. Всё это, а также любая другая потенциальная точка входа, доступная злоумышленнику, входит в формирование общей поверхности атаки организации.

Многие предприятия внедряют решения для управления поверхностью атаки (Attack Surface Management), которые помогают им взглянуть на свою систему безопасности со стороны [3]. Решения ASM сканируют цифровое присутствие компании так же, как это сделал

бы злоумышленник. В бизнесе всегда будут существовать уязвимости и атаки нулевого дня, требующие незамедлительного устранения. Однако сотрудники службы информационной безопасности могут сделать это только в той части IT-инфраструктуры, о которой они осведомлены и которую активно отслеживают. Применяя надежные методы управления уязвимостями, предприятия получают возможность минимизировать количество известных им систем, подвергающихся атакам.

Всё это можно изобразить с помощью диаграммы Эйлера-Венна, показанной на рисунке 1. Левый круг с красными квадратами – это множество «неизвестных и незащищённых» информационных активов компании. Правый круг с зелёными треугольниками – это множество «известных и защищённых» активов. Пересечение кругов с синими шестиугольниками – это множество «известных и незащищённых» активов. Предоставляя предприятиям возможность взглянуть на поверхность атаки со стороны, ASM помогает переместить информационные активы компании из категории «неизвестные и незащищённые» в категорию «известные и незащищённые», а затем выполнить приоритизацию и определить порядок перемещения активов в категорию «известные и защищённые». Или, другими словами, это помогает специалистам по информационной безопасности выбрать самый быстрый путь снижения информационных рисков компании, обнаруживая неизвестные активы и исправляя в первую очередь те системы, которые подвергаются наибольшей опасности.

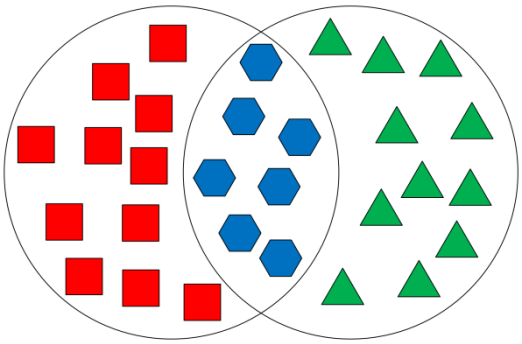

**Рис. 1.** Диаграмма Эйлера-Венна, отображающая различные множества информационных активов компании

**Зарубежные решения**

Для поддержания информационной безопасности организации на высоком уровне на международном рынке представлены различные инновационные решения.

*Randori (IBM)*

В 2022 году компания IBM приобрела Randori [4], ведущего поставщика услуг по управлению поверхностями атак. Randori была основана в 2018 году «хакерами в белых шляпах».

Преимущество системы ASM от Randori состоит в том, что она может предоставлять полную информацию о поверхности атаки из облака без развертывания какого-либо программного обеспечения на стороне клиента [5]. Кроме того, она позволяет внедрять принцип циклического и непрерывного улучшения рабочего процесса (во многом похожий на спарринг с злоумышленником) для улучшения и проверки защиты на итеративной основе. Как правило, этот процесс состоит из четырех этапов. Во-первых, обнаружение неизвестных информационных активов компании. Во-вторых, получение более глубокого представления о них и понимание их функциональной роли. В-третьих, определение приоритетности данных целей для злоумышленника. В-четвёртых, проведение тестирования для подтверждения эффективности действий по устранению уязвимостей.

Компания также предоставляет предприятиям решение Randori Platform [6], которое уникальным образом сочетает управление поверхностью атаки (Randori Recon) с непрерывной автоматизированной деятельностью «красной команды» (Red Team), применяющей в своей работе в том числе и стресс-тесты (Randori Attack). Одной из важных особенностей Randori является идея постоянного совершенствования ASM. Это даже отражено в названии

компании, так как термин «рандори» обозначает в японских боевых искусствах «практикуй, как ты сражаешься». Attack Surface Management от компании Randori становится лучше с каждой новой обнаруженной уязвимостью и с каждым новым разработанным планом её нейтрализации. Команда Randori учится и приспосабливается к клиентам, помогает им принимать более активные меры для обнаружения неизвестных уязвимостей. Всё это даёт возможность заказчику лучше определять приоритеты выявленных уязвимостей и качественнее проверять свою защиту в режиме реального времени, в результате чего сотрудники службы информационной безопасности смогут заранее выявить потенциально возможное место следующей атаки.

Для начала работы с Attack Surface Management от компании Randori клиенту нужно предоставить лишь адрес электронной почты и согласие руководства организации. Главное окно ASM Randori представлено на рисунке 2.

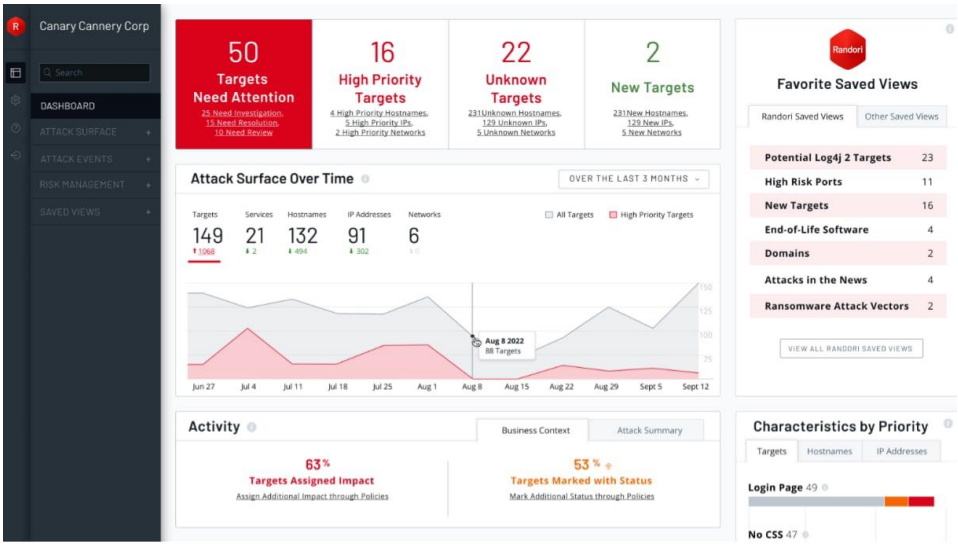


**Рис. 2.** Главное окно ASM Randori

*Mandiant (Google)*

В конце 2021 года компания Mandiant приобрела Intrigue.io ASM [7], а в начале 2022 года выпустила продукт Mandiant Attack Surface Management. В середине 2022 года Mandiant была куплена компанией Google [8], но сохранила бренд Mandiant.

Каждое подключение к сети нового оборудования в организации увеличивает её поверхность атаки. Если компания не сможет видеть все свои цифровые активы, то специалисты по информационной безопасности не смогут обнаружить потенциально возможные угрозы и неисправленные уязвимости. Mandiant Attack Surface Management позволяет получить контроль над всей IT-инфраструктурой компании. ASM анализирует внешние активы организации, как известные, так и неизвестные, и постоянно отслеживает их на предмет риска.

Сначала ASM отображает цифровые активы компании таким образом, чтобы обеспечить максимально широкий и глубокий обзор поверхности атаки. Attack Surface Management также анализирует активы предприятия, в том числе размещенные у партнеров и поставщиков. Затем ASM обогащает эту аналитическую информацию с помощью более 250 интегрированных источников данных и инструментов безопасности [9]. В итоге, руководство компании сможет узнать, чем владеет организация, как работает IT-инфраструктура и каким рискам она подвергается.

Далее Mandiant Attack Surface Management отслеживает сеть компании для обнаружения изменений и уязвимостей в режиме реального времени. ASM выявляет потенциальные угрозы безопасности, указывая, где отображённые активы могут быть уязвимы для известных угроз. Наконец, Attack Surface Management был специально разработан для поддержки динамических и распределенных информационных технологий. ASM легко интегрируется с процессами обеспечения безопасности организации и предоставляет полезную информацию,

адаптированную к тому, как работают сотрудники службы информационной безопасности. Специалисты смогут увидеть всё в режиме реального времени и вовремя устранять риски. На весну 2022 года уже более 4 тысяч организаций использовало преимущества Mandiant Attack Surface Management для усиления существующих мер контроля безопасности. Главное окно Mandiant ASM представлено на рисунке 3.


**Рис. 3.** Главное окно ASM Mandiant

*Cortex Xpanse (Palo Alto Networks)*

В конце 2020 года Palo Alto Networks приобрела компанию Expanse [10], чтобы расширить возможности портфеля продуктов Cortex для кибербезопасности. Новый продукт получил название Cortex Xpanse, который защищает крупнейшие организации мира, обнаруживая и отслеживания каждый актив компаний, имеющийся в сети Интернет.

Palo Alto Networks предоставляет организациям полную информацию обо всём, чем они владеют, включая IP-адреса, домены, сертификаты и другие облачные ресурсы. ASM Cortex Xpanse даёт компаниям возможность ознакомиться с цифровыми активами, чтобы они смогли защитить свою поверхность атаки локально, в облаке и по всей цепочке поставок. Cortex Xpanse был разработан управлением перспективных исследовательских проектов Министерства обороны США (DARPA) для одной из крупнейших ведомственных сетей в мире – сети Министерства обороны США [11]. В настоящее время Cortex Xpanse от Palo Alto Networks является одной из ведущих платформ управления поверхностью атаки. В отличии от других компаний, Palo Alto Networks собирает данные из записей DNS, регистраторов доменов, данных регистрации бизнеса и других источников, чтобы не только всесторонне изучить их, но и также точно идентифицировать каждый интернет-активов компаний. Cortex Xpanse использует это с целью выполнения интеллектуальной интернет-инвентаризации, уникальной для конкретной организации. ASM Cortex Xpanse обнаруживает неизвестные активы без необходимости что-либо устанавливать или настраивать. С помощью интеллектуальной инвентаризации всех известных и неизвестных активов организации, ASM сможет уменьшить поверхность атаки и сократить среднее время обнаружения и восстановления, а также обеспечить соблюдение политик облачной безопасности, что поможет компании повысить эффективность и рентабельность инвестиций в существующие системы безопасности. Главное окно ASM Cortex Xpanse представлено на рисунке 4.

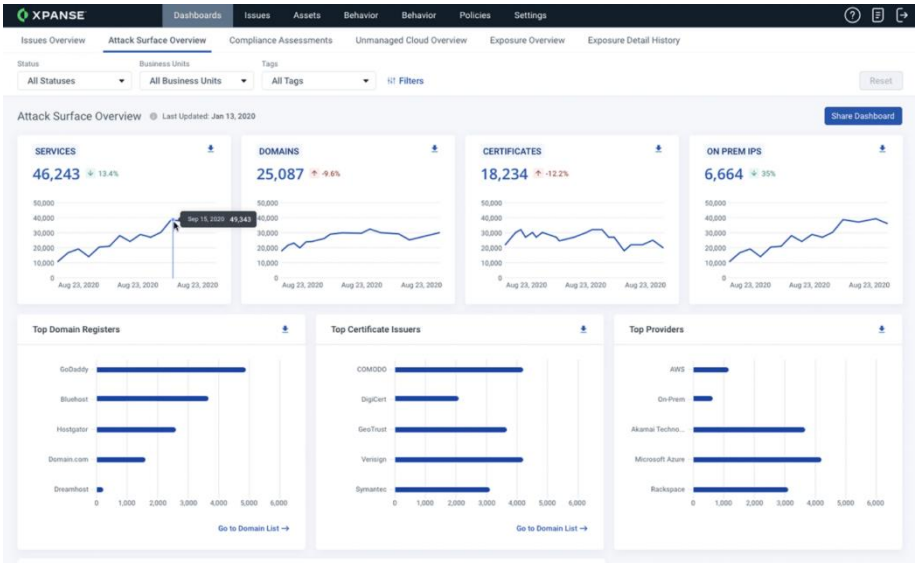


**Рис. 4.** Главное окно ASM Cortex Xpanse

**Отечественные решения**

Для обеспечения высокого уровня информационной безопасности организации на российском рынке представлен продукт Attack Surface Management компании F.A.C.C.T. (ранее Group-IB [12]), включенный в реестр отечественного программного обеспечения (запись в реестре от 20.05.2022 №13536) [13]. На весну 2023 года данный продукт является единственным российским решением ASM.

Attack Surface Management – это SaaS-решение (программное обеспечение как услуга), которое использует данные кибербразведки и отслеживает все доступные извне цифровые активы компании. Также ASM сопоставляет данные продукта Threat Intelligence компании F.A.C.C.T. (выполняющего разведку киберугроз) с подтверждённой заказчиком инфраструктурой предприятия [14]. Это позволяет точно оценить риски, задать приоритет действиям по реагированию и заметно увеличить показатели защищённости организации.

Продукт Attack Surface Management является относительно недорогим решением, поэтому его можно использовать как в небольшой компании, так и в крупной корпорации. Attack Surface Management является облачным решением, то есть не требует изменение инфраструктуры предприятия и установки дополнительного программного и аппаратного обеспечения. Это позволяет не нарушать бизнес-процессы. Для начала работы продукта нужно только указать сайт компании. Через 24 часа в Attack Surface Management на главной странице появятся оценки по десятибалльной шкале следующих параметров инфраструктуры организации:

1) уязвимости – не стоят последние обновления программного обеспечения;

2) сетевая безопасность – есть лишние открытые порты;

3) утечки – утечки учётных данных, связанных с выявленными цифровыми активами;

4) вредоносные программы – на периметре присутствует вредоносное программное обеспечение;

5) упоминания в дарквебе – уведомления о том, что на организацию готовится атака;

6) безопасность SSL/TLS сертификатов – поиск истёкших сертификатов;

7) почтовая безопасность – выявление некорректных настроек;

8) DNS и домены – проверка работоспособности и настроек DNS.

Также продукт найдёт SSL сертификаты, домены и IP-адреса, которые могут быть связаны с компанией [14]. В случае ложного срабатывания можно убрать лишние IP-адреса или добавить правильные.

Продукт позволяет наглядно увидеть распределение инфраструктуры организации по всему миру. Если компания считает, что все её активы находятся только в России, а Attack

Surface Management показывает, что они есть в других странах, то это значит, что к компании кто-то подключился извне.

Преимущества Attack Surface Management:

1. Быстрая скорость работы – для получения первых результатов требуется всего 24 часа.

2. Подходит для любой организации – продукт эффективно работает при любом размере инфраструктуры.

3. Легко пилотировать – не требует установки дополнительного программного и аппаратного обеспечения и остановки бизнес-процессов.

4. Защищает постоянно меняющийся периметр организации – легко подстраивается под новые условия при расширении инфраструктуры организации.

5. Дополняет аудит, минимизирует «серые зоны» между аудитами – позволяет проводить проверки между аудитами, так как качественные аудиты дороги и проводятся нечасто.

6. Для управления не нужны высококлассные специалисты – понять результаты работы продукта может любой сотрудник IT-отдела организации.

7. Уменьшает количество инцидентов, которые приходят на поверхности атаки организации – экономит время сотрудников отдела безопасности, так как фокусирует их внимание только на сложных атаках.

8. Цена лицензии на продукт рассчитывается по числу IP-адресов и доменов и действует один год без учёта изменения инфраструктуры.

Таким образом, продукт Attack Surface Management российской компании F.A.C.C.T. помогает защищать внешний периметр, который достаточно быстро и сильно размывается, в следствие чего становится очень сложно следить за активами предприятия. Организация чаще всего использует сторонние облачные решения, например, электронная почта, сервера базы данных. Компания не всегда может их контролировать, но она должна знать, что там происходит и какие риски возможны. Attack Surface Management позволяет со всем этим справиться, обеспечивая полную видимость внешней поверхности атаки. Главное окно ASM от компании F.A.C.C.T. представлено на рисунке 5.


**Рис. 5.** Главное окно ASM F.A.C.C.T.

**Сравнение зарубежных и отечественных решений.** В таблицах 1, 2 и 3 приводится сравнение продуктов Attack Surface Management, рассмотренных ранее. В данных таблицах представлена информация о технических возможностях доступных решений и об их основных характеристиках, определяющих потенциальное влияние на бизнес [15].

**Таблица 1.**

Позиционирование продуктов ASM

| | Сегмент рынка | | Модель развертывания | |
|---|---|---|---|---|
| | Малый бизнес | Средний и крупный бизнес | SaaS | Гибридная |
| ASM (F.A.C.C.T.) | ++ | ++ | ++ | – |
| Randori (IBM) | ++ | +++ | ++ | ++ |
| Mandiant (Google) | + | +++ | ++ | – |
| Cortex Xpanse (Palo Alto Networks) | + | +++ | ++ | – |

**Таблица 2.**

Сравнение ключевых критериев ASM

| | Гибкость в обнаружении активов | Активная оценка | Конвергентная защита | Внутренний ASM | Оценка рисков | Классификация активов |
|---|---|---|---|---|---|---|
| ASM (F.A.C.C.T.) | ++ | ++ | +++ | – | +++ | +++ |
| Randori (IBM) | ++ | ++ | +++ | ++ | +++ | +++ |
| Mandiant (Google) | +++ | ++ | ++ | – | ++ | +++ |
| Cortex Xpanse (Palo Alto Networks) | +++ | ++ | ++ | +++ | ++ | +++ |

**Таблица 3.**

Сравнение метрик оценки ASM

| | Расширяемость | Частота обнаружения | Лицензирование | Пользовательский опыт |
|---|---|---|---|---|
| ASM (F.A.C.C.T.) | ++ | ++ | +++ | +++ |
| Randori (IBM) | +++ | +++ | +++ | +++ |
| Mandiant (Google) | ++ | +++ | ++ | +++ |
| Cortex Xpanse (Palo Alto Networks) | +++ | +++ | ++ | +++ |

Показатели оценки каждого продукта:
«+++» – отличный показатель;
«++» – хороший показатель;
«+» – удовлетворительный показатель;
«–» – показатель отсутствует.

Из сравнения видно, что отечественный продукт ASM от компании F.A.C.C.T. не уступает зарубежным решениям. Он также имеет высокие показатели, доступную цену, гибкое лицензирование и понятный механизм оценки рисков.

**Заключение.** В современном мире, из-за быстрого роста IT-инфраструктуры, организации всё чаще будут сталкиваться с угрозами своим информационным активам. В отличие от традиционных средств защиты информации, таких как сканеры уязвимостей, которые не способны обнаружить ошибки в конфигурации облачных ресурсов, или проведение тестирований на проникновение, которое стоит очень дорого и проводится нерегулярно, продукты Attack Surface Management лишены этих недостатков. Благодаря автоматизированному и непрерывному процессу обнаружения активов и оценки рисков, продукты ASM экономят дра-

гоценное время специалистов по информационной безопасности, которые, благодаря знанию всей инфраструктуры компании, смогут более оперативно устранять уязвимости. Таким образом, применение решений Attack Surface Management поможет компании сохранить свои цифровые активы в безопасности, обеспечить непрерывную видимость поверхности атаки, обнаружить любые неправильные конфигурации или уязвимые компоненты IT-инфраструктуры и понять, как потенциальный противник может попытаться их использовать.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. What is an attack surface? [Электронный ресурс]. – Режим доступа: URL: https://www.ibm.com/topics/attack-surface (дата обращения: 18.05.2023).

2. CVE-2021-44228 [Электронный ресурс]. – Режим доступа: URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228 (дата обращения: 18.05.2023).

3. What is attack surface management? [Электронный ресурс]. – Режим доступа: URL: https://www.ibm.com/topics/attack-surface-management (дата обращения: 18.05.2023).

4. IBM Tackles Growing Attack Surface Risks with Plans to Acquire Randori [Электронный ресурс]. – Режим доступа: URL: https://newsroom.ibm.com/2022-06-06-IBM-Tackles-Growing-Attack-Surface-Risks-with-Plans-to-Acquire-Randori (дата обращения: 18.05.2023).

5. Randori Attack Surface Management [Электронный ресурс]. – Режим доступа: URL: https://www.randori.com/solutions/asm (дата обращения: 18.05.2023).

6. Randori Platform [Электронный ресурс]. – Режим доступа: URL: https://www.randori.com/platform (дата обращения: 18.05.2023).

7. Mandiant Adds Attack Surface Management to its SaaS Portfolio with the Acquisition of Intrigue [Электронный ресурс]. – Режим доступа: URL: https://www.mandiant.com/company/press-releases/mandiant-adds-attack-surface-management-its-saas-portfolio-acquisition (дата обращения: 18.05.2023).

8. Google Completes Acquisition of Mandiant [Электронный ресурс]. – Режим доступа: URL: https://www.mandiant.com/company/press-releases/google-completes-mandiant-acquisition (дата обращения: 18.05.2023).

9. Mandiant Advantage Attack Surface Management [Электронный ресурс]. – Режим доступа: URL: https://www.mandiant.com/advantage/attack-surface-management (дата обращения: 18.05.2023).

10. Palo Alto Networks Completes Acquisition of Expanse [Электронный ресурс]. – Режим доступа: URL: https://www.paloaltonetworks.com/company/press/2020/palo-alto-networks-completes-acquisition-of-expanse (дата обращения: 18.05.2023).

11. Continuously discover, evaluate, and mitigate attack surface risk [Электронный ресурс]. – Режим доступа: URL: https://www.paloaltonetworks.com/cortex/cortex-xpanse/attack-surface-management (дата обращения: 18.05.2023).

12. Это факт: российский бизнес Group-IB выкуплен локальным менеджментом, F.A.C.C.T. – новый̆ бренд кибербезопасности [Электронный ресурс]. – Режим доступа: URL: https://www.facct.ru/media-center/press-releases/facct (дата обращения: 18.05.2023).

13. Group-IB Attack Surface Management [Электронный ресурс]. – Режим доступа: URL: https://reestr.digital.gov.ru/reestr/745507/?sphrase_id=3008780 (дата обращения: 18.05.2023).

14. Attack Surface Management – Полный контроль внешней поверхности атаки [Электронный ресурс]. – Режим доступа: URL: https://www.facct.ru/products/attack-surface-management/ (дата обращения: 18.05.2023).

15. GigaOm Radar for Attack Surface Management [Электронный ресурс]. – Режим доступа: URL: https://research.gigaom.com/report/gigaom-radar-for-attack-surface-management-2 (дата обращения: 18.05.2023).

## REFERENCES

1. What is an attack surface? [Electronic resource]. – Access Mode: URL: https://www.ibm.com/topics/attack-surface (date of access: 05/18/2023).

2. CVE-2021-44228 [Electronic resource]. – Access mode: URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228 (date of access: 05/18/2023).

3. What is attack surface management? [Electronic resource]. – Access Mode: URL: https://www.ibm.com/topics/attack-surface-management (date of access: 05/18/2023).

4. IBM Tackles Growing Attack Surface Risks with Plans to Acquire Randori [Electronic resource]. – Access Mode: URL: https://newsroom.ibm.com/2022-06-06-IBM-Tackles-Growing-Attack-Surface-Risks-with-Plans-to-Acquire-Randori (date of access: 05/18/2023).

5. Randori Attack Surface Management [Electronic resource]. – Access mode: URL: https://www.randori.com/solutions/asm (date of access: 05/18/2023).

6. Randori Platform [Electronic resource]. – Access mode: URL: https://www.randori.com/platform (date of access: 05/18/2023).

7. Mandiant Adds Attack Surface Management to its SaaS Portfolio with the Acquisition of Intrigue [Electronic resource]. – Access Mode: URL: https://www.mandiant.com/company/press-releases/mandiant-adds-attack-surface-management-its-saas-portfolio-acquisition (date of access: 05/18/2023).

8. Google Completes Acquisition of Mandiant [Electronic resource]. – Access mode: URL: https://www.mandiant.com/company/press-releases/google-completes-mandiant-acquisition (date of access: 05/18/2023).

9. Mandiant Advantage Attack Surface Management [Electronic resource]. – Access mode: URL: https://www.mandiant.com/advantage/attack-surface-management (date of access: 05/18/2023).

10. Palo Alto Networks Completes Acquisition of Expanse [Electronic resource]. – Access mode: URL: https://www.paloaltonetworks.com/company/press/2020/palo-alto-networks-completes-acquisition-of-expanse (date of access: 05/18/2023).

11. Continuously discover, evaluate, and mitigate attack surface risk [Electronic resource]. – Access mode: URL: https://www.paloaltonetworks.com/cortex/cortex-xpanse/attack-surface-management (date of access: 05/18/2023).

12. It's a fact: the Russian business of Group-IB was bought out by local management, F.A.C.C.T. – a new brand of cybersecurity [Electronic resource]. – Access mode: URL: https://www.facct.ru/media-center/press-releases/facct (date of access: 05/18/2023).

13. Group-IB Attack Surface Management [Electronic resource]. – Access mode: URL: https://reestr.digital.gov.ru/reestr/745507/?sphrase_id=3008780 (date of access: 05/18/2023).

14. Attack Surface Management - Full control of the external attack surface [Electronic resource]. – Access mode: URL: https://www.facct.ru/products/attack-surface-management (date of access: 05/18/2023).

15. GigaOm Radar for Attack Surface Management [Electronic resource]. – Access mode: URL: https://research.gigaom.com/report/gigaom-radar-for-attack-surface-management-2 (date of access: 05/18/2023).

### Информация об авторах

*Станислав Павлович Киргизбаев* – студент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: s.p.kirgizbaev@gmail.com

*Владислав Павлович Киргизбаев* – аспирант, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: v.p.kirgizbaev@gmail.com

*Александр Алексеевич Бутин* – к.ф.-м.н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: butin_aa@mail.ru

**Authors**

*Stanislav Pavlovich Kirgizbaev*– student of the Department of Information Systems and Information Security, Irkutsk State Transport University, Irkutsk, e-mail: v.p.kirgizbaev@gmail.com

*Vladislav Pavlovich Kirgizbaev*– post-graduate student, Irkutsk State Transport University, Irkutsk, e-mail: v.p.kirgizbaev@gmail.com

*Alexander Alekseevich Butin* – Cand. Sc. (Physics and Mathematics), Associate Professor of the Department of Information Systems and Information Security, Irkutsk State Transport University, Irkutsk, e-mail: butin_aa@mail.ru

**Для цитирования**

С. П. Киргизбаев, В. П. Киргизбаев, А. А. Бутин. Применение решений Attack Surface Management для автоматизации мониторинга информационной безопасности в корпоративной сети // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2023. – №2(18). – С.7-16 – DOI: 10.26731/2658-3704.2023.2(18).7-16 – Режим доступа: http://ismm-irgups.ru/toma/218-2023, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 17.06.2023)

**For citations**

S. P. Kirgizbaev, V. P. Kirgizbaev, A. A. Butin. Application of attack surface management solutions for automation of information security monitoring in the corporate network // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: elektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2023. No. 2(18). P. 7-16. DOI: 10.26731/2658-3704.2023.2(18).7-16 [Accessed 17/06/23]