Оригинальная статья / Original article

УДК 004.072

https://doi.org/10.21869/2223-1560-2025-29-1-96-106

Модель поверхности атак для сложных систем на основе микросервисной архитектуры

В. Г. Миронова [1] ✉

[1] Московский институт электроники и математики им. А.Н. Тихонова (Национальный исследовательский университет «Высшая школа экономики»), ул. Мясницкая, д. 20, г. Москва 101000, Российская Федерация

✉ e-mail: vgmironova@hse.ru

Резюме

Цель исследования: *повышение уровня безопасности информации, обрабатываемой в информационных системах, основанных на микросервисной архитектуре; путём создания эффективной системы защиты, спроектированной на знаниях, полученных в результате создания модели поверхности атак.*

Методы. *В ходе проведения анализа были рассмотрены виды информационных систем (ИС), среди них выделены сложные ИС, созданные на основе микросервисной архитектуры. Рассмотрены российские и иностранные технологии, программное обеспечение, позволяющие автоматизировать процесс обработки информации. Предложена теоретико-множественная модель построения поверхности атаки для информационных систем, построенных на основе микросервисной архитектуры.*

Результаты. *Предложен оригинальный подход к описанию вектора и поверхности атаки, включающие в себя перечень часто встречающихся уязвимостей, способов и инструментов реализации атаки, а также перечень возможных объектов воздействия. Разработана теоретико-множественная модель построения поверхности атаки для информационных систем, построенных на основе микросервисной архитектуры.*

Заключение. *Проведение исследования и разработка модели поверхности атак для сложных ИС, построенных на микросервисной архитектуре, позволят повысить уровень знаний в области информационной безопасности (ИБ) и обеспечить безопасность обрабатываемых данных, путём построения эффективной системы защит информации, учитывающей актуальные угрозы и методы воздействия на ИС.*

Ключевые слова: *поверхность атаки; безопасность; тактика; техника; уязвимость.*

Конфликт интересов: *Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Миронова В. Г. Модель поверхности атак для сложных систем на основе микросервисной архитектуры // Известия Юго-Западного государственного университета. 2025; 29(1): 96-106. https://doi.org/10.21869/2223-1560-2025-29-1-96-106.

Поступила в редакцию 21.12.2024 *Подписана в печать 07.02.2025* *Опубликована 14.04.2025*

Attack surface model for complex systems based on microservice architecture

Valentina G. Mironova [1] ✉

[1] Moscow Institute of Electronics and Mathematics named after A.N. Tikhonov (National Research University Higher School of Economics), 20, Myasnitskaya str., Moscow 101000, Russian Federation

✉ e-mail: vgmironova@hse.ru

Abstract

Purpose of research. *Increasing the level of security of information processed in information systems based on microservice architecture; by creating an effective protection system designed on the basis of knowledge obtained as a result of creating an attack surface model.*

Methods. *During the analysis, types of information systems (IS) were considered, among them complex IS created on the basis of microservice architecture were highlighted. Russian and foreign technologies, software allowing to automate the process of information processing were considered. A set-theoretic model of constructing an attack surface for information systems built on the basis of microservice architecture was proposed.*

Results. *An original approach to the description of the attack vector and surface is proposed, including a list of frequently encountered vulnerabilities, methods and tools for implementing an attack, as well as a list of possible objects of influence. A set-theoretic model for constructing an attack surface for information systems built on the basis of a microservice architecture is developed.*

Results. *Conducting research and developing an attack surface model for complex information systems built on a microservice architecture will improve the level of knowledge in the field of information security (IS) and ensure the security of processed data by building an effective information security system that takes into account current threats and methods of influencing the information system.*

Keywords*. attack surface; security; tactics; technique; vulnerability.*

Conflict of interest. *The Author declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Mironova V. G. Attack surface model for complex systems based on microservice architecture // *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2025; 29(1): 96-106 (In Russ.). https://doi.org/10.21869/2223-1560-2025-29-1-96-106.

Received 21.12.2024 *Accepted 07.02.2025* *Published 14.04.2025*

***

Введение

В современном мире достаточно остро стоит вопрос обеспечения безопасности в активах организаций. Это связано прежде всего с тем, что технологии проникают во все сферы нашей деятельности.

Информационные системы (ИС) по структуре, наличию интеграции, функциональности можно разделить на простые и сложные. Простые ИС не могут обеспечивать достаточный уровень поддержки бизнес-процессов крупных и быстрорастущих компаний. Кроме того,

такие ИС плохо масштабируемы, сложны при интеграции. Простые ИС обычно разрабатываются для решения конкретных задач и имеют ограниченный функционал. Стоит отметить, что простые ИС зачастую представлены в виде монолитных решений, а, следовательно, для них характерно отсутствие гибкости. Монолитная архитектура представляет собой подход к разработке ИС, при котором приложение рассматривается как единое целое. Все компоненты системы, включая пользовательский интерфейс, бизнес-логику и работу с базой данных, тесно связаны и функционируют в рамках одного процесса.

Сложные ИС, в отличие от простых, обладают широким спектром функций, включая автоматизацию операций, анализ данных и поддержку принятия решений. Такие системы обычно включают в себя множество компонентов, таких как: базы данных, сети, пользовательские интерфейсы и бизнес-приложения. Сложные ИС преимущественно построены на основе микросервисной архитектуры. Такие системы легко масштабируемы. С помощью сложных ИС возможно реализовать решения задач по автоматизации сложных бизнес-процессов в компаниях и в целом можно говорить про возможность обработки большого объема данных. Микросервисная архитектура позволяет сложным ИС быть гибкими при внесении в них изменений и проведении различных интеграций.

На рис. 1 схематично представлена монолитная и микросервисная архитектура ИС.

Обеспечение ИБ обязательно для всех видов систем. Она включает широкий спектр программно-технических, а также иных решений, направленных на защиту от киберугроз.

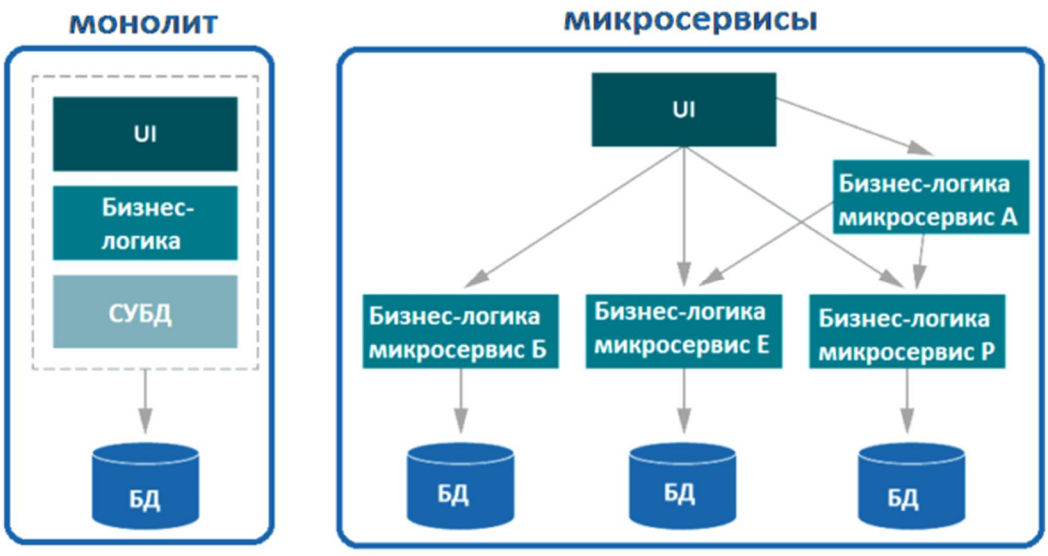

Рис. 1. Монолитная и микросервисная архитектура ИС

Fig. 1. Monolithic and micro-service architecture of IC

В [1] под киберугрозой принято считать потенциально возможное событие, действие, которое может нарушить бизнес-процесс или состояние защищенности информационного актива.

Под активом принято понимать сущность, имеющую ценность для компании, использующуюся для достижения целей компании, являющуюся объектом защиты и атаки с целью нарушения свойств безопасности (конфиденциальности, целостности и доступности).

Любое преднамеренное или непреднамеренное действие, которое нарушает, ограничивает или создаёт угрозу для нормального функционирования ИС, её конфиденциальности, целостности или доступности, можно отнести к атаке в контексте ИБ.

Преднамеренное действие, направленное на нарушение нормальной работы системы, её эксплуатацию или доступ к защищённой информации, можно отнести к атаке в контексте ИС.

В основном кибератаки – атаки, направленные на взлом компьютеров или серверов с использованием вредоносных программ, таких как вирусы, трояны и другие. Они могут привести к краже данных или получению контроля над устройством. Например, существуют программы-вымогатели, которые шифруют данные и требуют выкуп за их расшифровку. Также существуют атаки DoS и DDoS, которые перегружают систему запросами, делая её недоступной. DDoS-атаки сложнее обнаружить и защититься от них. APT-атаки представляют собой сложные и долгосрочные атаки на конкретные компании или организации с целью шпионажа или саботажа.

Физические атаки – атаки, направленные на элементы IT-инфраструктуры, такие как серверы, сети и коммуникационные каналы. Они могут привести к краже оборудования или повреждению линий связи или устройств.

В [2-4] приведены основные этапы кибератаки, которые включают в себя: разведку, подготовку средств кибератаки, первоначальный доступ/инициацию доступа, исполнение, закрепление, повышение привилегий, сокрытие действий, доступ к учетным данным, исследование, боковое перемещение, сбор данных, управление и контроль, утечку данных и влияние.

Под поверхностью атаки принято понимать количество потенциально уязвимых объектов компьютерной системы [5]. В целом термин «Поверхность атаки» может применяться для оценки ресурсов, потраченных на обеспечение безопасности системы, сети или конкретного устройства.

Для одного и того же устройства или программы может существовать несколько векторов атаки. Также в одной атаке могут использоваться разные векторы.

В целом под вектором атаки понимается путь, способ или средство, с помощью которого киберпреступники проникают в целевую систему. К векторам атаки могут относиться как действия и инструменты злоумышленников, так и человеческий фактор или уязвимые техно-

логии на стороне потенциальной жертвы и ее подрядчиков [6].

В задачу специалистов по защите информации входит уменьшение количества точек, образующих поверхность атаки. Например, в случае отключения открытого, но не используемого порта поверхность атаки будет уменьшена.

Материалы и методы

Результатом систематизированного метода анализа и описания всех возможных точек входа и направлений атак является модель поверхности атаки.

Рассмотрим теоретико-множественную модель поверхности атаки, описываемую следующим кортежем параметров:

$$AS=<AV,V>, \quad (1)$$

где AS (Attack Surface) – задает общие правила, согласно которым строится поверхность атаки; AV (Attack Vector) – множество векторов атак, V (vulnerability) – множество уязвимостей, присущих конкретно заданному объекту $V = \{v_1, v_2, \ldots, v_j\}$, где $j \in N$.

В Федеральном законе РФ от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» приведено понятие ИС. Под сложными ИС будем понимать системы:

– обладающие широким спектром функций, включая автоматизацию операций, анализ данных и поддержку принятия решений;

– включающие в себя множество компонент, таких как базы данных, сети, пользовательские интерфейсы и бизнес-приложения;

– построенные на микросервисной архитектуре.

Безусловно, использование сложных ИС для автоматизации бизнес-процессов и задач является приоритетным, поскольку сложные ИС могут быть интегрированы с внешними и уже существующими внутренними ИС. Кроме того, они отличаются модульностью, поскольку могут состоять из нескольких взаимонезависимых элементов (сервисов), которые легко заменяются и добавляются без необходимости полной модернизации системы. Стоит отметить, что сложные ИС, построенные на микросервисной архитектуре, гораздо проще масштабировать относительно систем, которые построены на монолитной архитектуре.

В состав сложной ИС входит:

– аппаратное обеспечение (серверы, рабочие станции, сетевое оборудование и другие физические устройства, которые обеспечивают функционирование системы);

– микросервисы;

– сетевая инфраструктура (сети, которые обеспечивают передачу данных между различными компонентами системы);

– данные, которые обрабатываются с помощью микросервисов;

– пользовательские интерфейсы (графические интерфейсы, веб-интерфейсы и другие средства взаимодействия пользователей с ИС).

Существует множество инструментов, позволяющих сформировать перечень возможных сценариев реализации угроз информационной безопасности (ИБ) и описание векторов компьютерных атак для любой ИС.

В частности:

- MITRE ATT&CK (https: //attack.mitre.org/) – материал, созданный на основе реальных наблюдений, содержащий описание тактик, техник и процедур, которые могут использовать нарушители [7];
- CVE (Common Vulnerabilities and Exposures) стандартизированный каталог идентификаторов известных уязвимостей [8];
- STRIDE. Модель помогает определять различные типы угроз, классифицируя их как подделку (Spoofing), подделку данных (Tampering), отказ от действий (Repudiation), раскрытие информации (Information Disclosure), отказ в обслуживании (Denial of Service) и повышение привилегий (Elevation of Privileges) [9].
- PASTA. Процесс моделирования атак и анализа угроз (PASTA) описывает семь шагов для сопоставления политики кибербезопасности с бизнес-целями: определение целей, определение сферы применения, разложение приложения, анализ угроз, анализ уязвимостей, моделирование атак, анализ риска и воздействия [10].

Отдельно стоит отметить Банк данных угроз безопасности информации, созданный Федеральной службой по техническому и экспортному контролю (ФСТЭК России) и размещенный по адресу в сети Интернет: https://bdu.fstec.ru/threat/.

Маршрут или метод, который злоумышленник использует для реализации своих намерений – вектор атаки. Он определяет способ взаимодействия атакующего с объектом атаки с целью достижения поставленных задач.

Рассмотрим теоретико-множественную модель вектора атаки для сложной ИС следующим кортежем параметров:

$$AV = (F,S,O), \quad (2)$$

где AV (Attack Vector) – это совокупность множества векторов атак; F – множество уязвимых факторов; $F = \{f_1, f_2, \ldots, f_i\}$, где $i \in N$; S – множество инструментов для реализации атаки, $S = \{s_1, s_2, \ldots, s_k\}$, где $k \in N$; O – множество объектов для реализации атаки, $O = \{o_1, o_2, \ldots, o_f\}$, где $f \in N$.

На практике анализ векторов атак и моделирование поверхности атак является необходимым, поскольку для любой ИС важно построить адекватную систему защиты информации. Рассмотрим веб-приложение, схема которого представлена на рис. 2. Веб-приложение включает в себя следующие сервисы:

- «Подсистема взаимодействия с пользователем» используется для обеспечения взаимодействия пользователя с остальными сервисами приложения;
- «Личный кабинет» необходим для сохранения персональных данных пользователя и взаимодействия с сервисами корзины, оплаты и доставки;

• «Сервис авторизации» отвечает за присвоение учетной записи положенных ей привилегий;

• «Корзина» используется для добавления пользователем необходимых товаров из каталога и перехода к сервису оплаты;

• «Товары» – каталог всех товаров интернет-магазина;

• «Оплата» используется для оплаты товаров, добавленных в корзину;

• «Доставка» помогает пользователю оформить доставку купленных товаров до места проживания.

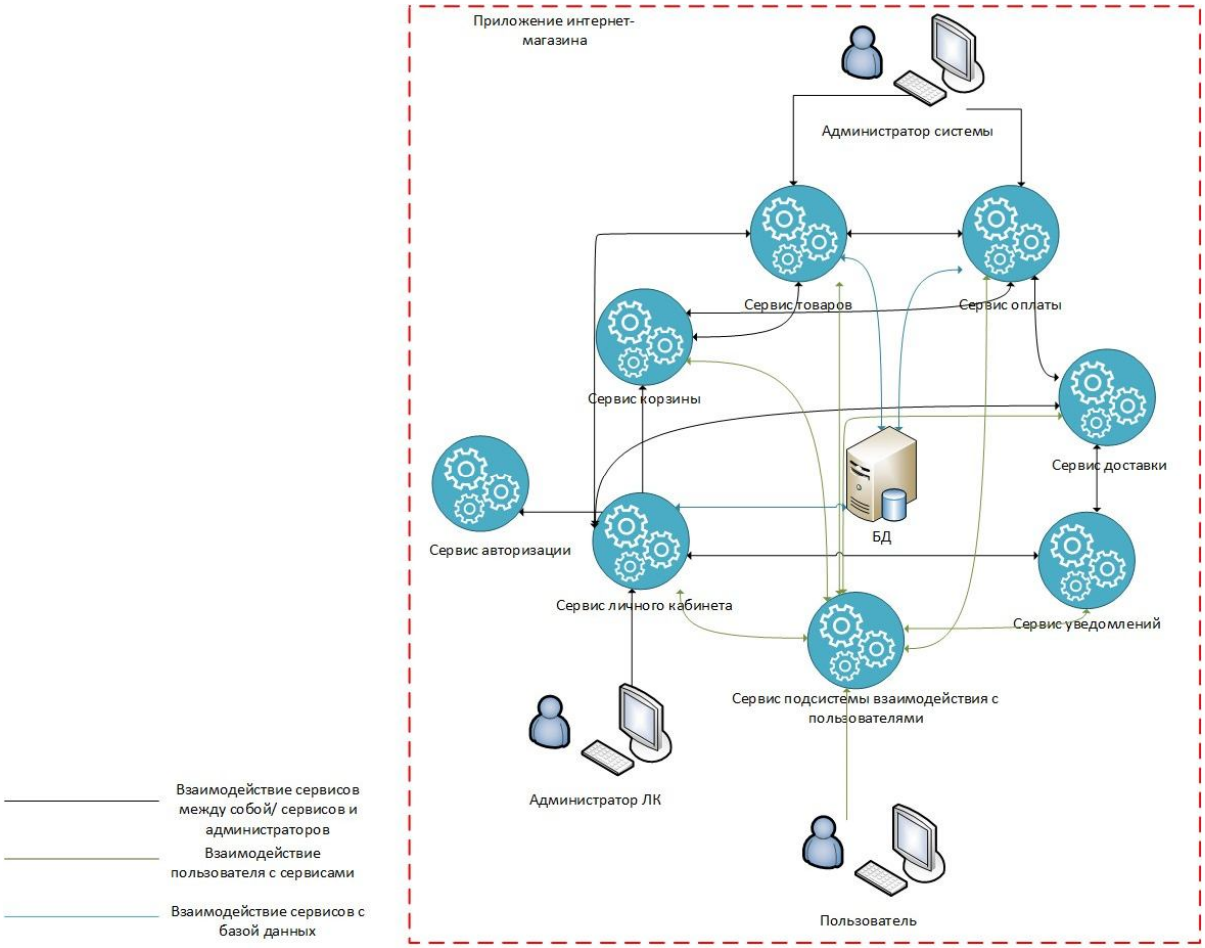

Рис. 2. Схема веб-приложения

Fig. 2. Web Application diagram

Для сервиса «Личный кабинет» в общем виде выделим объекты для реализации атаки:

– информация о пользователе (o_1);

– технические средства (o_2);

– структурные связи и программная среда (o_3);

– средства защиты информации (o_4).

В качестве инструментов реализации атаки в общем виде рассмотрим:

– вредоносное программное обеспечение (ПО) (s_1);

– программная закладка (s_2);

– сканирование трафика (s_3).

Под уязвимыми факторами будем понимать:

– отсутствие антивирусного ПО на компьютере пользователя (f_1);

– низкий уровень знаний в области ИБ персонала, обслуживающего систему (f_2);

– использование недоверенного ПО (f_3).

Вектор атаки для сервиса «Личный кабинет» вида $AV1 = (o_1, s_1, f_1)$ говорит о том, что на информацию о пользователе, обрабатываемую в сервисе, возможна атака с использованием уязвимости вида «Отсутствие антивирусного ПО на компьютере пользователя» посредством использования вредоносной программы [11, 12, 13-18].

Результаты и их обсуждение

Знания, полученные в ходе построения модели поверхности атаки и анализа векторов атак, позволяют усилить безопасность любой ИС путем устранения этих векторов и поддержания системы защиты информации в актуальном состоянии.

Выводы

Использование оригинального подхода к описанию вектора и поверхности атаки, который включает в себя возможность рассмотрения часто встречающихся уязвимостей, способов и инструментов реализации атаки, а также перечень возможных объектов воздействия, позволяет выявить возможные негативные факторы воздействия на ИС [19]. Определение векторов атак и построение моделей атак позволит спроектировать надёжную и эффективную систему защиты информации для сложных ИС.

Список литературы

1. Что такое Threat Intelligence и как применять? URL: http://www.sberbank.ru/ru/person/kibrary/articles/chto_takoe_threat_intelligence (дата обращения 10.11.2024).

2. Целевые атаки: этапы, инструменты, методы. URL: http://www.sberbank.ru/ru/ person/kibrary/articles/celevye-ataki-ehtapy-instrumenty-metody (дата обращения 10.11.2024).

3. Этапы проведения кибератак методы. URL: https://vasexperts.ru/blog/ bezopasnost/etapy-provedeniya-kiberatak/ (дата обращения 10.11.2024).

4. Связанные одной цепью: Kill Chain – этапы кибератак и как их предотвратить – URL: https://securitymedia.org/info/svyazannye-odnoy-tsepyu-kill-chain-etapy-kiberatak-i-kak-ikh-predotvratit.html (дата обращения 10.11.2024).

5. Подходы к оценке поверхности атаки и фаззингу веб-браузеров. URL: https://cyberleninka.ru/article/n/podhody-k-otsenke-poverhnosti-ataki-i-fazzingu-veb-brauzerov (дата обращения 10.11.2024).

6. Вектор атаки. URL: https://encyclopedia.kaspersky.ru/glossary/attack-vector/ (дата обращения 10.11.2024).

7. MITRE ATT&CK. URL: https://attack.mitre.org/ (дата обращения 10.11.2024).

8. CVE. URL: https://cve.mitre.org/ (дата обращения 10.11.2024).

9. Адаптация подхода S.T.R.I.D.E. для моделирования угроз. URL: https://osday.ru/2022/presentations/Moiseev.pdf (дата обращения 10.11.2024).

10. PASTA Threat Modeling. URL: https://threat-modeling.com/pasta-threat-modeling/ (дата обращения 10.11.2024).

11. Крупные кибератаки и утечки первой половины 2024 года в России. URL: https://blog.cortel.cloud/2024/05/23/krupnye-kiberataki-i-utechki-pervoj-poloviny-2024-goda-v-rossii/ (дата обращения: 15.10.2024).

12. Разработка архитектуры киберполигона для повышения качества и результативности учебного процесса в исследовании атак на информационные системы и сети Г. А. Остапенко, С. С. Куликов, А. В. Коноплин, А. А. Остапенко // Информация и безопасность. 2023. Т. 26. № 1. С. 101-108. https://doi.org/10.36622/VSTU.2023.26.1.012.

13. Демьянов А. Тестирование кибербезопасности встроенных систем с помощью их цифрового двойника // Электроника: наука, технология, безопасность. 2021. № 7 (208). С. 126−29.

14. Ульянов А.Н., Столяров М.Г., Стельмах И.В. Качество плюс наглядность применение технологий виртуализации вычислительных ресурсов в информационно-образовательной среде // ВВО. 2021. № 6 (33).

15. Монахов М.Ю., Тельный А.В., Мишин Д.В. О возможностях использования киберполигонов в качестве оценочных средств определения уровня сформированности компетенций // Информационное противодействие угрозам терроризма. 2015. Т. 1, № 25. С. 269-277.

16. НКЦКИ: существует угроза кибератак на российские информационные ресурсы // Интернет-портал по информационной безопасности в сети. 2022. URL: https://safesurf.ru/specialists/news/675925/ (дата обращения: 15.10.2024).

17. «Лаборатория Касперского»: количество киберинцидентов в российских компаниях увеличилось в 4 раза // «Лаборатория Касперского» : [сайт]. 2022. URL: https://www. kaspersky.ru/about/press-releases/2022_laboratoriya-kasperskogokolichestvo-kiberincidentov-v-rossijskih-kompaniyah-uvelichilos-v-4- raza (дата обращения: 15.10.2024).

18. Монахов М.Ю., Тельный А.В., Мишин Д.В. О возможностях использования киберполигонов в качестве оценочных средств определения уровня сформированности компетенций // Информационное противодействие угрозам терроризма. 2015. Т. 1, № 25. С. 269-277.

19. Архангельский О.Д., Сютов Д.В., Кузнецов А.В. Практические подходы к созданию инфраструктуры индустриального киберполигона // Автоматизация в промышленности. 2020. № 1. С. 52−57.

References

1. What is Threat Intelligence and how to use it? (In Russ.). Available at: http:// www.sberbank.ru/ ru/person/kibrary/articles/chto_takoe_threat_intelligence (accessed 10.11.2024).

2. Targeted attacks: stages, tools, methods. (In Russ.). Available at: http://www.sberbank.ru/ ru/person/ kibrary/articles/celevye-ataki-ehtapy-instrumenty-metody (accessed 10.11.2024).

3. Stages of cyber attacks methods. (In Russ.). Available at: https://vasexperts.ru/ blog/bezopasnost/ etapy-provedeniya-kiberatak/ (accessed 10.11.2024).

4. Linked by one chain: Kill Chain - stages of cyber attacks and how to prevent them. (In Russ.). Available at: https://securitymedia.org/info/svyazannye-odnoy-tsepyu-kill-chain-etapy-kiberatak- i-kak-ikh-predotvratit.html (accessed 10.11.2024).

5. Approaches to assessing the attack surface and fuzzing web browsers. (In Russ.). Available at: https://cyberleninka.ru/article/n/podhody-k-otsenke-poverhnosti-ataki-i-fazzingu-veb-brauzerov (accessed 10.11.2024).

6. Attack vector. (In Russ.). Available at: https://encyclopedia.kaspersky.ru/ glossary/attack-vector/ (accessed 10.11.2024).

7. MITRE ATT&CK. Available at: https://attack.mitre.org/ (accessed 10.11.2024).

8. CVE. Available at: https://cve.mitre.org/ (accessed 10.11.2024).

9. Adaptation of the S.T.R.I.D.E. approach for threat modeling. (In Russ.). Available at: https://osday.ru/2022/presentations/Moiseev.pdf (accessed 11/10/2024).

10. PASTA Threat Modeling. Available at: https://threat-modeling.com/pasta-threat-modeling/ (accessed 10.11.2024).

11. Major cyberattacks and leaks in the first half of 2024 in Russia. (In Russ.). Available at: https://blog.cortel.cloud/2024/05/23/krupnye-kiberataki-i-utechki-pervoj-poloviny-2024-goda-v-rossii/ (accessed 15.10.2024).

12. Ostapenko G. A., Kulikov S. S., Konoplin A. V., Ostapenko A. A. Development of cyber polygon architecture to improve the quality and effectiveness of the educational process in the study of attacks on information systems and networks. *Informatsiya i bezopasnost = Information and security*. 2023; 26(1): 101-108. (In Russ.). https://doi.org/10.36622/ VSTU.2023.26.1.012.

13. Demyanov A. Testing the cybersecurity of embedded systems using their digital counterpart. *Elektronika: nauka, tekhnologiya, bezopasnost' = Electronics: science, technology, safety*. 2021; (7): 126-29. (In Russ.).

14. Ulyanov A.N., Stolyarov M.G., Stelmakh I.V. Quality plus visibility the use of virtualization technologies for computing resources in the information and educational environment. *BBO.* 2021; (6). (In Russ.).

15. Monakhov M.Yu., Telny A.V., Mishin D.V. On the possibilities of using cyber polygons as assessment tools for determining the level of competence formation. *Informatsionnoe protivodeistvie ugrozam terrorizma = Information counteraction to terrorist threats*. 2015; 1(25): 269-277 (In Russ).

16. NCC: There is a threat of cyber attacks on Russian information resources. *An online information security portal on the web*. 2022 (In Russ). Available at: https://safesurf.ru/ specialists/news/675925 / (accessed: 10/15/2024).

17. Kaspersky Lab: the number of cyber incidents in Russian companies has increased 4 times. *Kaspersky Lab: [website]*. 2022. (In Russ). Available at: https://www. kaspersky.ru/ about/press-releases/2022_laboratoriya-kasperskogokolichestvo-kiberincidentov-v-rossijskih-kompaniyah-uvelichilos-v-4 - raza (accessed: 10/15/2024).

18. Monakhov M.Yu., Telny A.V., Mishin D.V. On the possibilities of using cyber ranges as assessment tools for determining the level of competence development. *Informatsionnoe protivodeistvie ugrozam terrorizma = Information counteraction to terrorist threats*. 2015; 1(25): 269-277 (In Russ).

19. Arkhangelsky O.D., Syutov D.V., Kuznetsov A.V. Practical approaches to creating the infrastructure of an industrial cyberpolygon. *Avtomatizatsiya v promyshlennosti = Automation in industry.* 2020; (1): 52-57. (In Russ.).

Информация об авторе / Information about the Author

Миронова Валентина Григорьевна,
кандидат технических наук, доцент кафедры информационной безопасности киберфизических систем, Московский институт электроники и математики им. А.Н. Тихонова (Национальный исследовательский университет «Высшая школа экономики»), г. Москва, Российская Федерация, e-mail: vgmironova@hse.ru

Valentina G. Mironova, Cand. of Sci. (Engineering), Associate Professor of Information Security of Cyber-Physical Systems Department, Moscow Institute of Electronics and Mathematics named after A.N. Tikhonov (National Research University Higher School of Economics), Moscow, Russian Federation, e-mail: vgmironova@hse.ru