ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.627:504.064.36:519.688

DOI: 10.21822/2073-6185-2023-50-4-148-157 Оригинальная статья / Original article

Организация реагирования на инциденты информационной безопасности

Д.О. Трофимов[1], М.С. Шепелев[1], С.А. Резниченко[1,2,3]
[1]Финансовый университет при правительстве Российской Федерации,
[1]25993, г.Москва, Ленинградский пр–кт, 49, Россия,
[2]Национальный исследовательский ядерный университет «МИФИ»,
[2]115409, г.Москва, Каширское шоссе, 31, Россия,
[3] Российский государственный гуманитарный университет,
[3]125047, г. Москва, Миусская площадь, д. 6, Россия

Резюме. Цель. Разработка практических рекомендаций для создания эффективной системы реагирования на инциденты информационной безопасности (ИБ). **Метод**. Исследование основано на существующих методах и инструментах обнаружения и анализа инцидентов ИБ, а также последствий таких инцидентов и их влияния на работу компании или организации. **Результат**. Разработан комплекс практических рекомендаций, направленных на создание эффективной системы реагирования на инциденты информационной безопасности (ИБ). Выявлены наиболее эффективные и адаптированные подходы, включающие как технические средства обнаружения, так и процессы оперативного реагирования на инциденты. Рекомендации созданы с учетом особенностей компаний и организаций различных отраслей, а также предполагаются для использования лицами, не обладающими глубокими знаниями в области информационной безопасности. Рекомендации включают понятные пошаговые инструкции, ресурсы и советы, которые позволят компаниям легко внедрять предложенные меры в своей практике. **Вывод**. Разработка эффективной системы реагирования на инциденты ИБ является критически важной для компаний и организаций, так как они сталкиваются с растущим числом кибератак и угроз информационной безопасности. Создание эффективной системы реагирования на инциденты ИБ является неотъемлемой частью успешной бизнес-стратегии. Разработанные практические рекомендации обладают потенциалом существенно уменьшить риски и ущерб, связанные с ИБ, даже для компаний и организаций без предварительного опыта в данной области. Рекомендации сосредотачиваются не только на технических аспектах, но и на организационных мероприятиях, чтобы обеспечить своевременное обнаружение, анализ и реагирование на инциденты.

Ключевые слова: информационная безопасность, инцидент, обнаружение, реагирование, анализ, угроза

Для цитирования: Д.О. Трофимов, М.С. Шепелев, С. А. Резниченко. Организация реагирования на инциденты информационной безопасности. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(4):148-157. DOI:10.21822/2073-6185-2023-50-4-148-157

Organization of response to information security incidents

D.O. Trofimov[1], M.S. Shepelev[1], S.A. Reznichenko [1,2,3]
[1]Financial University under the government of Russian Federation,
[1]49 Leningradsky Ave., Moscow 125993, Russia,
[2]National Research Nuclear University “MEPhI”, (Moscow Engineering Physics Institute),
[2] 31 Kashirskoe highway, Moscow 115409, Russia,
[3]Russian State University for the Humanities,
[3]6 Miusskaya Square, Moscow 125047, Russia

Abstract. **Objective**. Development of practical recommendations for creating an effective information security incident response system. **Method**. The article includes an analysis of existing methods and tools for detecting and analyzing information security incidents, as well as a study of the consequences of such incidents and their impact on the work of a company or organization. **Result**. Development of a set of practical recommendations aimed at creating an effective information security incident response system. During the analysis of existing methods and tools for the detection and analysis of information security incidents, the most effective and adapted approaches were identified. These methods include both technical means of detection and rapid incident response processes. The recommendations were created taking into account the characteristics of companies and organizations of various industries and are also intended for use by persons who do not have deep knowledge in the field of information security. The recommendations include clear step-by-step instructions, resources and tips that will allow companies to easily implement the proposed measures in their practice. **Conclusion**. The development of an effective information security incident response system is critically important for companies and organizations, as they face an increasing number of cyber-attacks and threats to information security. Creating an effective information security incident response system is an integral part of a successful business strategy. The developed practical recommendations have the potential to significantly reduce the risks and damage associated with information security, even for companies and organizations without prior experience in this field. These recommendations focus not only on technical aspects, but also on organizational measures to ensure timely detection, analysis and response to incidents.

Keywords: Information security, reaction, analyse, threat, detection, incident

For citation: D.O. Trofimov, M.S. Shepelev, S.A. Reznichenko. Organization of response to information security incidents. Herald of Daghestan State Technical University. Technical Sciences. 2023; 50(4): 148-157. DOI:10.21822/2073-6185-2023-50-4-148-157

Введение. В современном информационном обществе безопасность информации играет важную роль. Каждый день компании и организации сталкиваются с угрозами информационной безопасности, такими как вирусы, хакерские атаки, утечки данных и другие инциденты, которые могут привести к непредсказуемым последствиям.

Для борьбы с такими угрозами важно иметь готовность к реагированию на инциденты информационной безопасности. Согласно ГОСТ Р ИСО/МЭК ТО 18044-2007 [1]: инцидент информационной безопасности — появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ. Также Российская компания Kaspersky даёт определение реагирования на инциденты информационной безопасности — в мире информационной безопасности так называют комплекс мероприятий по обнаружению и прекращению кибератаки или утечки данных из инфраструктуры организации и устранению последствий [2].

Организация реагирования на инциденты информационной безопасности является важной частью общей стратегии информационной безопасности компании или организации. Однако, несмотря на внедрение типовых политик информационной безопасности и применение защитных мер, невозможно обеспечить абсолютную защиту информации, информационных систем, сервисов и сетей.

Всегда существует вероятность наличия уязвимостей, которые могут сделать защиту информационной безопасности неэффективной, и, следовательно, возможность возникновения инцидентов информационной безопасности. Такие инциденты могут оказывать негативное воздействие на бизнес-процессы организации как прямым, так и косвенным образом. Более того, всегда будут появляться новые, ранее неизвестные угрозы. Если конкретная организация не готова должным образом реагировать на такие инциденты,

это может привести к неэффективной реакции и усилить отрицательное влияние на бизнес.

Постановка задачи. В данной работе рассматриваются основные принципы и подходы к организации реагирования на инциденты ИБ, анализируются существующие методы и инструменты для обнаружения и анализа инцидентов ИБ, исследуются последствия инцидентов ИБ и их влияние на работу компании/организации, а также на основе вышесказанного разрабатываются рекомендации по созданию эффективной системы обнаружения и реагирования на инциденты ИБ.

Методы исследования. Для любой организации, которая ответственно относится к информационной безопасности, важно использовать структурный и плановый подход к:

1. Обнаружению, оповещению и оценке инцидентов информационной безопасности: необходимо иметь механизмы и процессы для обнаружения и оперативного оповещения о возникновении инцидентов. Кроме того, проводится оценка и анализ инцидентов для понимания их характеристик и последствий.
2. Реагированию на инциденты информационной безопасности: в случае возникновения инцидентов применяются соответствующие защитные меры с целью предотвращения или уменьшения негативных последствий. Важно также планировать и проводить меры по восстановлению после инцидентов, а также обеспечивать непрерывность бизнес-процессов.
3. Извлечению уроков из инцидентов информационной безопасности: на основе опыта и анализа инцидентов принимаются меры по внедрению превентивных защитных мер, чтобы предотвратить подобные инциденты в будущем. Также важно улучшать общий подход к управлению инцидентами информационной безопасности, опираясь на полученные знания и опыт.

Для достижения вышеуказанных целей менеджмент инцидентов ИБ подразделяют на четыре отдельных этапа, аналогично циклу PDCA (Plan, Do, Check, Act), методологии принятия решения, используемой в управлении качеством. Также известен как цикл Деминга: планирование и подготовка; использование; анализ; улучшение. Рассмотрим каждый этап:

Планирование и подготовка: на данном этапе следует создать или обновить существующие политики ИБ, связанные с реагированием на инциденты. Также следует создать в организации соответствующее структурное подразделение с заданными обязанностями и ответственностью или же нанять компанию уже с готовым решением по данному вопросу, например SOC (SOC (Security operations center) - структурное подразделение организации, отвечающее за оперативный мониторинг IT-среды и предотвращение киберинцидентов.

Также Компания Kaspersky даёт следующее определение данному этапу - разработка плана реагирования на инциденты, который включает в себя сценарии работы сотрудников при наступлении того или иного ИБ-события, список необходимых ресурсов, перечень применяемых инструментов, права и обязанности команды реагирования. Также к этапу подготовки относится обучение ответственных за реагирование на инцидент сотрудников. Этот этап не привязан к конкретному инциденту [2].

Использование: при использовании системы менеджмента инцидентов ИБ необходимо осуществить следующие процессы:

1. Обнаружение и оповещение о возникающих событиях ИБ (посредством анализа системы человеком или использования различных систем, например SIEM (SIEM (Security Information and Event Management) - это решение, которое позволяет организациям обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб бизнесу;
2. Обогащение, фильтрацию и нормализацию событий, чтобы определить, какие события можно отнести к категории инцидентов ИБ;
3. Реагирование на инцидент ИБ;
4. Необходимо предоставлять информацию о случившемся инциденте ИБ и

все соответствующие детали персоналу внутри своей организации, а также сотрудникам сторонних организаций.

5. Провести правовую экспертизу;
6. Провести запись всех действий и решений для последующего анализа.

Анализ: после устранения инцидента ИБ необходимо извлечь и изучить информацию из инцидента, определить улучшения, которые могут быть внедрены в меры информационной безопасности, и использовать эту информацию для улучшения системы управления инцидентами информационной безопасности в целом.

Улучшение: улучшения проводятся на основе данных из проведённого анализа или современных тенденций в мире. Этап «Улучшение» включает в себя пересмотр результатов анализа уже произошедших инцидентов ИБ, а также на основе анализа рисков информационной безопасности и менеджмента организации.

Также производится улучшение системы управления инцидентами информационной безопасности и ее документации. В этом процессе инициируются улучшения в области безопасности, включая внедрение новых или обновленных мер информационной безопасности. Это позволяет организации адаптироваться к изменяющимся угрозам и повысить эффективность своих мероприятий по обеспечению безопасности информации (рис1.).

Рис. 1. Основное содержание менеджмента инцидентов информационной безопасности [2]
Fig. 1. Main contents of information security incident management [2]

Также компания Kaspersky дополняет этап «Использование» следующими пунктами:

- Идентификация. Собственно, реагирование на инцидент начинается с обнаружения кибератаки или утечки данных. На этом этапе поступает оповещение об инциденте, специалисты оценивают угрозу и собирают данные о ней. Обычно процесс идентификации сводится к изучению логов.

- Сдерживание. Команда реагирования принимает меры для пресечения распространения угрозы. К ним может относиться изоляция пораженных устройств, изоляция затронутых сегментов сети, временное отключение интернета и так далее. Одна из дополнительных целей этого этапа — не допустить уничтожения следов атаки, которые потребуются при расследовании.

- Ликвидация — устранение угрозы, удаление вредоносных файлов, смена паролей

пострадавших учетных записей, восстановление утраченных данных и так далее.

- Возвращение к работе — ввод обратно в эксплуатацию систем, затронутых инцидентом, подключение устройств к сети, тестирование и мониторинг корректности их работы [2].

В настоящее время существует множество методов и инструментов для обнаружения и анализа инцидентов ИБ. Они разделяются на автоматизированные и традиционные.

К традиционным можно отнести:

Журналы событий: сотрудник может анализировать журналов событий вручную. Журналы системных событий, сетевых устройств и приложений, могут помочь выявить необычную или потенциально вредоносную активность. Необходимо обращать внимание на аномалии, подозрительные попытки входа, ошибки аутентификации и другие события, которые могут указывать на инцидент ИБ.

Мониторинг сетевого трафика: анализируя сетевой трафик вручную, можно обнаружить аномалии, подозрительные пакеты или активность, которая отличается от обычного поведения. Это может помочь выявить потенциальные инциденты ИБ.

Анализ логов системы: ручной анализ логов системы, включая файлы журналов операционной системы и приложений, может помочь выявить аномалии, необычные действия или попытки несанкционированного доступа. Необходимо обращать внимание на ошибки, предупреждения или любую активность, которая не соответствует ожидаемому поведению.

Отчёты: обратите внимание на отчеты и сообщения от сотрудников или пользователей о подозрительной активности или необычном поведении системы.

Взаимодействие с другими специалистами по ИБ: сотрудничество с другими специалистами по информационной безопасности, обмен опытом и знаниями может помочь в обнаружении и анализе инцидентов ИБ.

В качестве автоматизированных систем рассмотрим SIEM, SOAR, EDR и UEBA:

1) SIEM — это система, накапливающая в себе все данные (журналы работы или, как говорят спецы, логи) от других средств защиты, умеющая понимать многие «форматы» логов из разных источников - средств защиты, быстро искать нужную информацию в этих логах, долгое время их хранить [3] SIEM-система (Security Event Management) — это объединение двух классов: SEM, который используется для мониторинга событий безопасности в реальном времени; SIM, который используется для анализа и хранения данных с различных объектов инфраструктуры организации. Основные задачи SIEM-систем:

- получение журналов с разнообразных средств защиты;
- приведение к единообразному формату (нормализация) полученных данных; классифицирование уже нормализованных сообщений в зависимости от их содержания, то есть таксономия нормализованных данных; корреляция классифицированных событий;
- создание инцидента, предоставление инструментов для проведения расследования
- хранение информации о событиях и инцидентах в течение длительного времени (от 6 месяцев);
- быстрый поиск по хранящимся в SIEM данным.

Для эффективной работы с системой управления информационной безопасностью (SIEM) специалист по ИБ должен иметь возможность быстро и удобно осуществлять поиск по предыдущим инцидентам и событиям, хранящимся в SIEM-системе.

Это позволяет специалисту получить дополнительные технические подробности для проведения расследования атаки или анализа произошедшего инцидента.

2) SOAR (Security Orchestration, Automation and Response) — класс программных продуктов, предназначенных для оркестровки систем безопасности, то есть их координации и управления ими. [4]

Решения класса SOAR позволяют собирать данные о событиях информационной безопасности из различных источников, обрабатывать их и автоматизировать типовые сценарии реагирования на них, тем самым избавляют специалистов по безопасности от необходимости управлять каждым из них в отдельности, и помогают сфокусироваться на анализе сложных инцидентов. Функциональные возможности: сбор данных о потенциальных инцидентах; анализ инцидента; идентификация и классификация угроз; реагирование на инциденты; визуализация данных и формирование отчетности.

На основе комплексного анализа полученных данных решение SOAR оценивает текущее состояние инфраструктуры и идентифицирует потенциально небезопасные события. Затем система классифицирует эти события в соответствии с их степенью риска и информирует специалистов о них. При необходимости SOAR может принимать автоматизированные меры, такие как изоляция зараженных устройств, чтобы предотвратить дальнейшее распространение атаки. Эти меры соответствуют политике безопасности компании и направлены на минимизацию угрозы для системы. После чего формирует полноценный отчёт о произошедшем инциденте.

1) EDR (Endpoint Detection & Response) - передовая система безопасности, которая объединяет различные компоненты для обеспечения безопасности конечных точек (Конечные точки — это компьютеры, ноутбуки, мобильные устройства и другие устройства, подключенные к сети). В отличие от традиционных решений безопасности, основанных на анализе паттернов и сигнатур, решения EDR отслеживают приток внешнего трафика и обрабатывают операции и действия фоновых процессов. Методы EDR анализируют журналы, созданные в результате серии действий, предпринятых злоумышленником перед началом полномасштабной атаки, и используют эти журналы и анализ для обнаружения вторжений и формирования защитных ответов. [5].

Эта технология решает проблему постоянного мониторинга и эффективного реагирования на сложные угрозы безопасности.

2) UEBA (User and Entity Behavior Analytics) - технология выявления киберугроз, основанная на анализе поведения пользователей, а также устройств, приложений и иных объектов в информационной системе. [6]

«Поведенческий анализ пользователей и сущностей» (UEBA) использует машинное обучение для моделирования поведения пользователей и сущностей, пытаясь обнаружить аномальное поведение, которое может быть признаком кибератаки. Решения UEBA обычно собирают информацию о среднем ожидаемом поведении пользователей и организаций из различных источников. Как только эта информация отфильтрована и предварительно обработана, можно установить базовую линию поведения пользователя с помощью шаблонов или отпечатков пальцев. Затем решения UEBA осуществляют непрерывный мониторинг поведения пользователей и организаций, чтобы сравнить его с базовым поведением. [7]

Мы рассмотрели основные существующие методы и инструменты для обнаружения и анализа инцидентов ИБ, однако их список на этом не ограничивается. Каждый из инструментов следует выбирать в соответствии с определённые условиями в организации.

Под инцидентом информационной безопасности (ИБ) понимается одно или серия нежелательных событий ИБ, которые имеют значительную вероятность компрометации бизнес-операций и угрожают информационной безопасности [1].

Такие события как: прерывания бизнес-процессов, нарушения конфиденциальности, целостности или доступности активов организации – являются последствия инцидентов ИБ, которые, в ходе реализации угроз могут возникнуть преднамеренно или случайно. Данные инциденты приводят к потере производительности и ущербу с точки зрения как материальных затрат, так и репутации [8].

Для оценки последствий инцидентов информационной безопасности необходимо идентифицировать возможные инциденты и разработать сценарии их развития.

В таких сценариях должны быть предусмотрены нежелательные события, вызывающие инциденты, а также защитные меры, которые могут предотвратить инциденты. Кроме того, необходимо учесть последствия инцидента, то есть конечные результаты или последствия инцидента. Для каждого сценария должны быть определены меры по предотвращению негативных событий информационной безопасности, меры по сдерживанию и устранению последствий инцидента, а также меры по восстановлению после него. [9]

По данным компании Positive Technologies самыми распространёнными категориями жертв являются [10]:

Госучреждения – 18%; промышленность – 13%; наука и образование – 7%; медицинские учреждения – 7%; транспорт – 6%; IT-компании – 5%; сфера услуг – 4%; блокчейн-проекты – 4%; другие – 36%

Также следует определить причину, по которой возникают инциденты ИБ в организациях: шпионаж с целью получения данных; финансовая выгода для злоумышленника; промежуточное звено (использование организации как инструмент для достижения иной цели); политика. Ещё компания Positive technologies выделяет следующие последствия инцидентов ИБ для организаций и частных лиц [11] (рис. 2).

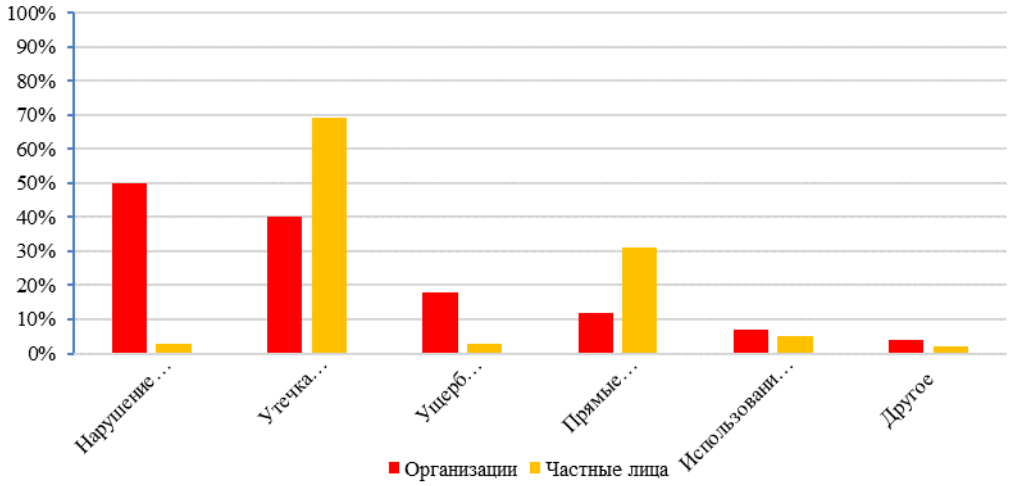

Рис. 2. Последствия инцидентов информационной безопасности
Fig. 2. Consequences of information security incidents

Следует отметить, что причины возникновения инцидентов информационной безопасности могут быть разнообразными и определяются целями злоумышленников. Важно понимать, что последствия таких инцидентов могут существенно отличаться и оказывать непосредственное влияние на организации. Понимание причин и последствий инцидентов информационной безопасности поможет организациям более осознанно и эффективно разрабатывать свои стратегии защиты и улучшать свою информационную безопасность [12,13].

Обсуждение результатов. Изучив рекомендации от различных компаний, организаций и интеграторов в сфере ИБ мы сделали вывод, что для создания эффективной системы обнаружения и реагирования на инциденты информационной безопасности рекомендуется принять следующие меры:

Мониторинг: необходимо разработать систему мониторинга, которая будет контролировать действия и события в информационной среде организации. Следует включить *мониторинг сетевого трафика*, *журналов событий*, *системных ресурсов* и других релевантных источников данных. Это поможет обнаружить подозрительные действия и аномалии.

Системы обнаружения угроз: нужно реализовать специализированные инструменты и

программное обеспечение для обнаружения и анализа потенциальных угроз информационной безопасности. Такие системы включают в себя различные средства для обнаружения угроз.

Сценарии и критерии: необходимо написать сценарии и определить критерии, которые будут служить основой для определения инцидентов информационной безопасности. Это поможет быстро обнаруживать инциденты ИБ, а также моментально реагировать на них, благодаря заранее определённым действиям по тому или иному сценарию.

Отдел по реагированию на инциденты: следует сформировать команду, которая будет отвечать за обнаружение, анализ и реагирование на инциденты информационной безопасности. Эта команда должна иметь достаточные знания и навыки в области информационной безопасности и быть готовой к оперативным действиям при возникновении инцидента. Она может быть как в составе организации, так и по найму. Чаще всего подобными решениями являются SOC или ГРИИБ (группа реагирования на инциденты ИБ)

План реагирования на инциденты: сценарии пишутся для автоматизированных решений по реагированию на инциденты. Однако оно может быть и традиционное – вручную, для этого как раз и нужны планы. Нужно разработать документированные планы реагирования на различные типы инцидентов, включить в них процедуры по обнаружению, исследованию, устранению и восстановлению после инцидента.

Аудиты и обновления: важно проводить регулярные аудиты системы обнаружения и реагирования на инциденты, чтобы убедиться в ее эффективности. Обновляйте системы и инструменты, следите за новыми угрозами и обновленными методами атак. Также следует проводить Pentest (тестирование на проникновение) - метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника , чтобы найти слабые места в системе, которые могут привезти к инцидентам ИБ.

Обучение сотрудников: не меньшим приоритетом является организация обучения и осведомления сотрудников об угрозах информационной безопасности, процедурах обнаружения и реагирования на инциденты. Следует регулярно напоминать о политиках и процедурах безопасности и обучать сотрудников правилам использования информационных ресурсов. Также при создании системы обнаружения и реагирования на инциденты информационной безопасности необходимо учитывать специфику организации, ее ресурсы и потребности.

Вывод. В данной статье мы разработали базовые рекомендации по созданию эффективной системы обнаружения и реагирования на инциденты ИБ. Обладая такой системой, организации могут не бояться кибератак, целью которых может быть утечка информации. Однако не стоит забывать, что создать абсолютно защищенную систему невозможно, а злоумышленники придумывают новые методы взлома и виды атак на компании.

Наше исследование сосредоточилось на анализе существующих методов и инструментов для обнаружения и анализа инцидентов ИБ, а также их последствий на работу компании или организации. Мы также уделили особое внимание разработке практических рекомендаций, которые будут доступны и понятны всем, а в частности организациям, не связанным с ИБ сферой.

Результаты исследования позволяют разработать простые и понятные рекомендации по созданию эффективной системы обнаружения и реагирования на инциденты ИБ, которые будут полезны для всех, в том числе для лиц, не связанных с областью информационной безопасности.

Наш подход имеет новизну в том, что он предлагает реальные практические рекомендации для создания эффективной системы реагирования на инциденты ИБ. Мы понимаем, что многие компании и организации могут не обладать необходимыми знаниями и навыками в области ИБ, и им сложно разбираться в технической документации. Поэтому мы стремимся предоставить понятные и удобные рекомендации, которые помогут им

выполнять свои бизнес-задачи без вреда для информационной безопасности.

Таким образом, данное исследование будет способствовать улучшению уровня защиты информации и снижению рисков, связанных с ИБ, в различных компаниях и организациях.

Библиографический список:

1. ГОСТ Р ИСО/МЭК ТО 18044–2007 - Национальный стандарт российской федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности (https://docs.cntd.ru/document/1200068822)
2. Реагирование на инциденты (Incident Response). // Электронная энциклопедия Касперского. URL: https://encyclopedia.kaspersky.ru/glossary/incident-response/ (дата обращения 16.05.23)
3. Рахметов Р. SIEM системы (Security Information and Event Management) - что это и зачем нужно? // Электронный блог компании Security Vision. URL: https://www.securityvision.ru/blog/siem-chto-eto-i-zachem-nuzhno/ (дата обращения: 16.05.23)
4. SOAR (Security Orchestration, Automation and Response). // Электронная энциклопедия Касперского. URL: https://encyclopedia.kaspersky.ru/glossary/security-orchestration-automation-and-response-soar/ (дата обращения: 17.05.23)
5. Na-Eun Park, Yu-Rim Lee, Soyoung Joo, So-Yeon Kim, So-Hui Kim, Ju-Young Park, Seo-Yi Kim, Il-Gu Lee. Performance evaluation of a fast and efficient intrusion detection framework for advanced persistent threat-based cyberattacks. //Международная база цитирования Science Direct. URL: https://www.sciencedirect.com/science/article/pii/S0045790622007637 (дата обращения: 18.05.23)
6. UEBA. // Электронная энциклопедия Касперского. URL: https://encyclopedia.kaspersky.ru/glossary/ueba/ (дата обращения: 19.05.23)
7. Alejandro G. Martín, Marta Beltrán, Alberto Fernández-Isabel, Isaac Martín de Diego. An approach to detect user behaviour anomalies within identity federations. //Международная база цитирования Science Direct. URL: https://www.sciencedirect.com/science/article/pii/S0167404821001802 (дата обращения: 18.05.23)
8. Писаренко И. Выявление инцидентов информационной безопасности. // Information security: сетевой журнал, URL: https://lib.itsec.ru/articles2/control/vyyavlenie-incidentov-informacionnoy-bezopasnosti (дата обращения: 19.05.23)
9. Щербакова А.Ю., Зефиров С.Л. Сценарии инцидента сбора информации // Материалы II Международной научно-практической конференции студентов и молодых ученых «Молодежь и наука: модернизация и инновационное развитие страны»: электронное научн. издание. - ФГУП НТЦ «Информрегистр», Депозитарий электронных изданий. - 2012. - С. 769-772.
10. Актуальные киберугрозы: II квартал 2022 года. // Электронный ресурс компании Positive Technologies, URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q2/ (дата обращения: 19.05.23)
11. Крючков А.В., Прус Ю.В., Резниченко С.А., Технологические основы национальной информационной безопасности // Сборник статей, Международной научно-практической конференции Российского государственного гуманитарного университета. 2018. С. 58-63.
12. Резниченко С.А., Сиротский А.А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов // Безопасность информационных технологий, 2021. Том.28, №3. С. 103–117.
13. Резниченко С.А., Дмитриева Т.В., Подкосов С.В., Евдокимов О.Г., Семухин С.Д. Проблемы управления информационной безопасностью в кредитно-банковской системе передачи данных // Московский экономический журнал. 2022. № 2. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-2-2022-36/ (дата обращения: 19.05.23)

References

1. GOST R ISO/IEC TO 18044–2007. National standard of the russian federation. Information technology. Methods and means of ensuring security. Information Security incident management (https://docs.cntd.ru/document/1200068822)
2. Incident Response. Kaspersky Electronic Encyclopedia. URL: https://encyclopedia.kaspersky.ru/glossary/incident-response/ (accessed 16.05.23)
3. Rakhmetov R. SIEM systems (Security Information and Event Management) - what is it and why is it needed? Electronic blog of Security Vision company. URL: https://www.securityvision.ru/blog/siem-chto-eto-i-zachem-nuzhno/ (accessed 16.05.23)
4. SOAR (Security Orchestration, Automation and Response). Kaspersky Electronic Encyclopedia. URL: https://encyclopedia.kaspersky.ru/glossary/security-orchestration-automation-and-response-soar/(accessed 17.05.23)
5. Na-Eun Park, Yu-Rim Lee, Soyoung Joo, So-Yeon Kim, So-Hui Kim, Ju-Young Park, Seo-Yi Kim, Il-Gu Lee. Performance evaluation of a fast and efficient intrusion detection framework for advanced persistent threat-based cyberattacks. International quotation Database Science Direct. URL: https://www.sciencedirect.com/science/article/pii/S0045790622007637 (accessed 18.05.23)

6. UEBA. Kaspersky Electronic Encyclopedia. URL: https://encyclopedia.kaspersky.ru/glossary/ueba/ (accessed 19.05.23)
7. Alejandro G. Martín, Marta Beltrán, Alberto Fernández-Isabel, Isaac Martín de Diego. An approach to detect user behaviour anomalies within identity federations. // International quotation Database Science Direct. URL: https://www.sciencedirect.com/science/article/pii/S0167404821001802 (accessed 18.05.23)
8. Pisarenko I. Identification of information security incidents. // Information security. (In Russ) Available at:https://lib.itsec.ru/articles2/control/vyyavlenie-incidentov-informacionnoy-bezopasnosti (accessed 19.05.23)
9. Shcherbakova A.Y., Zefirov S.L. Scenarios of the information gathering incident. Materials of the II International Scientific and Practical Conference of students and young scientists "Youth and science: modernization and innovative development of the country": electronic scientific journal. edition. FSUE STC "Informregister", Depository of electronic publications. 2012; 769-772.
10. Current cyber threats: The second quarter of 2022. Electronic resource of Positive Technologies company, URL:https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q2/(accessed 19.05.23)
11. Kruchkov A.V., Prus Y.V., Reznichenko S.A., Technological foundations of national information security. *Collection of articles, International scientific and Practical Conference of the Russian State University for the Humanities*. 2018; 58-63.
12. Reznichenko S.A., Sirotskiy A.A. A formalized model of an organization's information security audit for compliance with the requirements of standards. *Information Technology Security,* 2021; 28(3):103-117.
13. Reznichenko S.A., Dmitrieva T.V., Podkosov S.V., Evdokimov O.G., Semuhin S.D. Problems of information security management in the credit and banking data transmission system // Moscow Economic Journal. 2022. №2 URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-2-2022-36/ (accessed 19.05.23)

Сведения об авторах:

Трофимов Даниил Олегович, студент направления подготовки «Информационная безопасность банковских автоматизированных систем»; daniil.trofimov.1986@mail.ru ORCID.org/ 0009-0005-2606-7734

Шепелев Матвей Сергеевич, студент направления подготовки «Информационная безопасность банковских автоматизированных систем»; matwey20031106@gmail.com ORCID.org/ 0009-0009-1800-8469

Резниченко Сергей Анатольевич, кандидат технических наук, доцент; rsa_5@bk.ru ORCID.org/0000-0002-1539-0457

Information about authors:

Daniil O. Trofimov, Student in the direction of training "Information security of automated banking systems"daniil.trofimov.1986@mail.ru ORCID.org/ 0009-0005-2606-7734 Matvey S. Shepelev, Student in the direction of training "Information security of automated banking systems"matwey20031106@gmail.com ORCID.org/ 0009-0009-1800-8469

Sergey A. Reznichenko, Cand.Sci.(Eng.), Assoc.Prof.; rsa_5@bk.ru ORCID.org/0000-0002-1539-0457

Конфликт интересов / Conflict of interest.

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

Поступила в редакцию/ Received 05.09.2023.

Одобрена после рецензирования / Reviced 30.09.2023.

Принята в печать /Accepted for publication 30.09.2023.