Басова А.Н. Концептуальный анализ современных подходов и программных инструментов обеспечения кибербезопасности // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 7(45) с. 104–114

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

КОНЦЕПТУАЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ И ПРОГРАММНЫХ ИНСТРУМЕНТОВ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Басова А.Н.
ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ (ИТМО)», Санкт-Петербург, Россия (197101, город Санкт-Петербург, Кронверкский пр-кт, д. 49 литер а) e-mail: nastya74.01@mail.ru

В статье приводится категориальный анализ современных, применяемых в отечественных коммерческих компаниях, концептуальных подходов к формированию стратегической концепции кибербезопасности и разработке структуры систем кибербезопасности с учетом соответствия данных подходов друг другу и используемым в компании программным инструментам защиты. Результатом работы является система иерархическая категоризация современных программных инструментов кибербезопасности и матрица соответствия концептуальных подходов, подходов к разработке структур систем кибербезопасности и категорий программных инструментов друг другу.

Ключевые слова: Информационная безопасность, кибербезопасность, программные инструменты, цифровая трансформация, сравнительный анализ, концептуальные подходы, матрица соответствия.

CONCEPTUAL ANALYSIS OF MODERN APPROACHES AND SOFTWARE TOOLS FOR CYBERSECURITY

Basova A.N.
NATIONAL RESEARCH UNIVERSITY OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS (ITMO), St. Petersburg, Russia (197101, St. Petersburg, Kronverkskiy pr-kt, 49, lit. a), e-mail: nastya74.01@mail.ru

The article provides a categorical analysis of modern conceptual approaches used in domestic commercial companies to form a strategic concept of cybersecurity and develop the structure of cybersecurity systems, taking into account the correspondence of these approaches to each other and the security software tools used in the company. The result of the work is a system of hierarchical categorization of modern cybersecurity software tools and a matrix of correspondence of conceptual approaches, approaches to the development of cybersecurity system structures and categories of software tools to each other.

Keywords: Information security, cybersecurity, software tools, digital transformation, comparative analysis, conceptual approaches, compliance matrix.

Введение

Начиная, с 2020 г. отечественная сфера кибербезопасности начала развиваться ускоренными темпами: начали появляются новые программные инструменты, подходы, что связано с такими факторами как: массовая цифровизация и цифровая трансформация отечественных компаний [9, с. 166], сопровождающаяся появлением новых точек уязвимостей в информационных системах предприятий и усложнением ИТ-архитектуры предприятий [11, С. 34-36]; санкционный режим функционирования и последующие процессы массового технологического импортозамещения на фоне прекращения поддержки и сопровождения ряда

ПО, включая ПО в сфере кибербезопасности [12, с. 217]; увеличение количества и уровня организации кибератак [10, с. 36][4, с.150]; государственная поддержка разработок в сфере цифровых технологий [6, с.507]. Так, в начале 2024 г. рост рынка информационной безопасности составил 30-40%, при этом крупнейшие отечественные вендоры (Сбербанк, Kasperski) заявили о формировании качественно новых подходов к разработке инструментов киберзащиты.

На фоне быстрого развития и расширения применяемых подходов и инструментов [3, с.387], а также быстро меняющегося законодательства в сфере кибербезопасности отечественные компании ставят своей целью обеспечение сплошной киберзащиты с применением наиболее современных технологий (с применением ИИ на основе машинного обучения) [2, с.28], что с учетом нехватки оборудования, специалистов и превышением спроса над предложением значительно завышает бюджеты по информационной безопасности компаний. Так, за последние 5 лет отмечается двукратное увеличение расходов на кибербезопасность на отечественных предприятиях, при этом по данным исследования ГК InfoWatch в 2023 г. на 2% больше респондентов (48%) говорили о недостатке финансирования в сферу информационной безопасности на предприятиях.

Однако, сплошная защита это лишь один из концептуальных подходов и, следовательно, при применении не соответствующих инструментов она может быть неэффективной [8, с.193][7, с.142], что чаще всего связано с внедрения инструментов с дублированием функций и неконтролируемым увеличением сложности структуры киберсистем из-за отсутствия учета модульного характера существующих программных инструментов.

Целью исследования является формирование типовых концептуальных решений для коммерческих компаний в сфере кибербезопасности на основе учета соответствия применяемых программных инструментов кибербезопасности принятым в компании концептуальным подходам к проектированию и разработке систем кибербезопасности.

Современные концептуальные подходы к разработке систем кибербезопасности

В современных условиях одиночные инструменты киберзащиты уже не в состоянии обеспечить минимально необходимый уровень кибербезопасности [5, с. 7], поэтому коммерческие компании стремятся создавать и развивать многоуровневые системы защиты, охватывающие такие сферы как: контроль доступа к информации, защита конфиденциальности, защита от целевых атак, вирусная защита и т.д. [1, с. 91-92] Разработка концепции и структуры таких систем требует наличия комплексных подходов. В отечественной практике большинство данных подходов только начинают внедряться и использоваться коммерческими предприятиями, тем не менее, на данный момент можно выделить 3 развивающихся концептуальных подхода к формированию систем кибербезопасности:

1) Подход, ориентированный на зрелость (Maturity-based approach) или подход сплошная защиты – наиболее распространенный подход, нацеленный на достижение определенного уровня зрелости информационной системы безопасности в целом. Вероятность возникновения рисков не учитывается, вместо этого закрывается наибольшее количество рисков. Главное преимущество – ускоренные темпы развития кибербезопасности на предприятии, комплексное снижение информационных рисков, недостаток – неуправляемый рост контроля, неэффективное использование ресурсов. Чаще всего используется молодыми

компаниями догоняющего типа, быстро наращивающими масштабы своей деятельности, а также крупными компаниями в случае резкого увеличения объемов киберугроз или законодательного повышения требований к информационной защищенности.

2) Риск - ориентированный подход (Risk-based approach) – молодой подход, набирающий популярность среди отечественных компаний, нацеленный на отбор и приоритезацию наиболее вероятных рисков, при этом наименее вероятные и опасные риски могут быть полностью проигнорированы. Преимущество – эффективное распределение ресурсов, недостаток – сложности просчета рисков. На данный момент активно применяется средними и крупными компаниями, однако в связи с увеличением сложности и скоординированности атак на киберсистемы становится все менее эффективным и требуем методологического переосмысления.

3) Проактивный подход (Proactive approach) – самый молодой подход, находящийся на стадии формирования. Нацелен на трансформацию всей компании для внедрения передовых автоматических систем кибербезопасности и создание полноценной экосистемы для вовлечение всех участников бизнес- процессов: от сотрудников до клиентов и партнеров. Преимущество – обеспечение наивысшего уровня информационной безопасности, относительно низкие издержки на обслуживание, недостаток – необходимость реорганизации существующих процессов, дороговизна установки и настройки систем.

После выбора концептуального подхода выбирается подход к разработке структуры системы кибербезопасности. Укрупненно их можно разбить на 4 подхода:

1) Классический / традиционный подход: при данном подходе система кибербезопасности представлены одним или несколькими центрами мониторинга информационной безопасности (Security Operation Center, SOC), содержащими применяемый в компании набор информационных продуктов, каждый из которых имеет свою собственную функцию и не пересекается по функционалу с другими продуктами в SOC. Преимущественно применяется малыми и средними компаниями за счет простоты реализации.

2) Экосистемный подход: является развитием классического подхода, в отличие от которого предполагает отсутствие автономности информационных продуктов в пользу формирования эффекта синергии. Все продукты при таком подходе интегрированы между собой на всех этапах функционирования системы при помощи решений класса SOAR (Security Orchestration, Automation and Response), которые позволяют собирать и обрабатывать данные из всех подключенных информационных продуктов, а также осуществлять автоматизированные сценарии реагирования на угрозы. Является наиболее распространенным подходом к кибербезопасности на крупных предприятиях.

3) Результативный подход: развивает экосистемный подход благодаря дополнительному созданию единого центра противодействия угрозам, занимающегося преимущественно мониторингом и реагированием на катастрофические угрозы (как правило, не более 5-7 на компанию), и применению тестовой платформы, либо использованию существующих тестовых платформ, для выявления новых рисков и сценариев (Bug Bounty). Является наиболее молодым подходом, находящимся на начальном этапе внедрения в наиболее информационно зрелых компаниях.

4) Усиленный результативный подход: включает в себя все элементы результативного подхода, но вместо мониторинга концентрируется на развитие инфраструктуры предприятия, нацеленном на сокращение площади атаки и удлинении пути

продвижения хакеров (например, отключение серверов, сокращение количества портов и т.д.). Считается более эффективным чем обычный результативный подход, но сопряжен с дополнительными рисками, например, риск создания новых уязвимостей, снижения информационной эффективности компании, появление новых багов и сбоев и т.д.

Выбор концептуального подхода к формированию системы киберзащиты зависит от потребностей и возможностей компании. Не менее важна интерпретации и понимание этого подхода руководством компании. На основе отобранного концептуального подхода формируются принципы и направления развития киберсистем, а также выбирается или создается новый подход к разработке. В зависимости от интерпретации в рамках одного концептуального подхода возможно применение разных подходов к разработке, однако не все они будут совместимыми, то есть они не всегда будут соответствовать задачам, поставленным в концептуальном подходе: Таблица 1. При неучете данной совместимости эффективность проводимых мероприятия может быть значительно снижена.

Таблица 1 – Матрица совместимости концептуальных подходов и подходов к разработке

Концептуальный подход	Совместимые подходы к разработке
Подход, ориентированный на зрелость	Классический / традиционный подход Экосистемный подход Результативный подход Усиленный результативный подход
Риск - ориентированный подход	Классический / традиционный подход Экосистемный подход Результативный подход
Проактивный подход	Результативный подход Усиленный результативный подход

Современные программные инструменты кибербезопасности

На основе выбранного подхода к разработке систем кибербезопасности формулируются функциональные требования и начинается отбор программных инструментов. Для системности отбора важно понимать возможности и основные выполняемые инструментами задачи [8, С. 104-105], для этого все категории инструменты можно разбить на классы в соответствии с их сферой защиты (какие типы устройств, соединений защищает данный инструмент), функциональностью / модульностью (сколько функций / подсистем включает в свой состав данный инструмент), степенью автоматизации (какие задачи инструмент может выполнять в автоматическом режиме), уровнем использования ИИ / сложностью решаемых задач (какие угрозы инструмент в состоянии предотвратить в автоматическом режиме).

В рамках данной статьи выделены следующие критерии разбивка инструментов по классам: Таблица 2.

Таблица 2 – Критерии разбиения программных инструментов киберзащиты по классам

Критерий	Значения критериев
Сфера защиты	Конечные точки Сетевой трафик / Сеть Корпоративная информационная система в целом
Функциональность	Оповещение об инциденте Распознавание угроз Распознавание атак Реагирование на угрозы Предотвращение атак Изучение угроз Предоставление рекомендаций по кибербезопасности Долгосрочное хранение данных об инцидентах Восстановление систем Тестирование систем
Степень автоматизации	Автоматическое оповещение Автоматическое реагирование на угрозы Автоматическое изучение угроз Автоматическое формирование сводного отчета по совокупности систем безопасности Автоматическое управление другими системами безопасности Автоматическое восстановление систем
Сложность решаемых задач	Обычные / типовые угрозы Сложные / скрытые угрозы Целевые атаки

На основе отобранных критериев можно выделить следующие укрупненные классы:

1) **Базовые инструменты защиты конечных точек**
   a. Сфера защиты: конечные точки
   b. Функциональность: оповещение, распознавание угроз, реагирование на угрозы
   c. Степень автоматизации: оповещение, реагирование на угрозы
   d. Сложность решаемых задач: обычные / типовые угрозы
2) **Продвинутые инструменты защиты конечных точек**
   a. Сфера защиты: конечные точки
   b. Функциональность: оповещение, распознавание, изучение угроз, реагирование на угрозы, долгосрочное хранение информации об инцидентах
   c. Степень автоматизации: оповещение, реагирование на угрозы
   d. Сложность решаемых задач: обычные / типовые, сложные угрозы

3) **Инструменты анализа сетевого потока**
   a. Сфера защиты: сетевой трафик
   b. Функциональность: оповещение, распознавание угроз
   c. Степень автоматизации: оповещение
   d. Сложность решаемых задач: обычные / типовые, сложные угрозы
4) **Инструменты анализа и реагирования на события в сетевом трафике**
   a. Сфера защиты: сетевой трафик
   b. Функциональность: оповещение, распознавание реагирование на угрозы, изучение угроз долгосрочное хранение информации об инцидентах
   c. Степень автоматизации: оповещение, реагирование на угрозы
   d. Сложность решаемых задач: обычные / типовые, сложные угрозы
5) **Инструменты комплексного учета и анализа событий**
   a. Сфера защиты: корпоративная информационная система
   b. Функциональность: оповещение, распознавание угроз, атак, изучение угроз, долгосрочное хранение данных об инцидентах
   c. Степень автоматизации: оповещение, изучение, формирование сводного отчета по совокупности систем безопасности, управление другими системами безопасности
   d. Сложность решаемых задач: обычные / типовые, сложные угрозы, целевые атаки
6) **Инструменты комплексного учета и реагирования**
   a. Сфера защиты: корпоративная информационная система
   b. Функциональность: оповещение, распознавание угроз, атак, изучение угроз, долгосрочное хранение данных об инцидентах, реагирование на угрозы
   c. Степень автоматизации: оповещение, изучение, формирование сводного отчета по совокупности систем безопасности, управление другими системами безопасности реагирование на угрозы
   d. Сложность решаемых задач: обычные / типовые, сложные угрозы, целевые атаки
7) **Инструменты проактивной защиты**
   a. Сфера защиты: корпоративная информационная система
   b. Функциональность: все перечисленное
   c. Степень автоматизации: все перечисленное
   d. Сложность решаемых задач: обычные / типовые, сложные угрозы, целевые атаки

Таким образом, все современные типы программных инструментов защиты можно распределить по данным категориям: Рисунок 1.

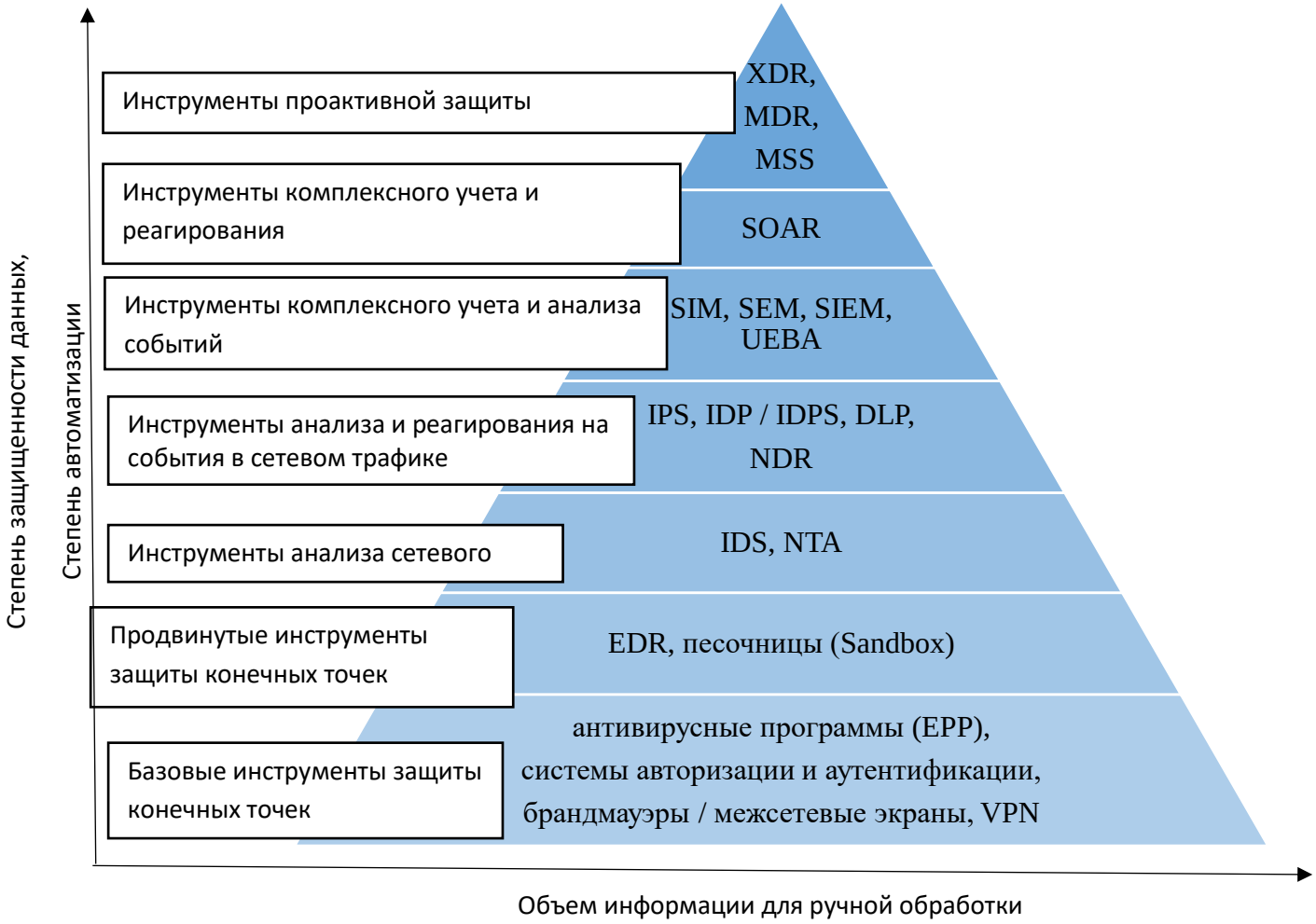

Рисунок 1 – Программные инструменты киберзащиты по категориям

На основе выделенных классов можно более наглядно отобразить рост сложности задач и функциональности инструментами по мере перехода из класса в класс, что обусловлено включением более низко ранговых инструментов в состав более высокоранговых. Так, например, инструменты типа XDR (Extended Detection and Response) включают в свой состав инструменты типов IDS, IPS, NTA, DLP, SIEM и т.п. (конкретный набор может отличаться в зависимости от производителя). Классы значительно легче отобрать в соответствии с выбранным компанией подходом к разработке системы кибербезопасности: Таблица 3.

Таблица 3 – Типовые решения на основе подхода к разработке и класса инструмента кибербезопасности

Подход к разработке	Требования подхода к инструментам	Классы инструментов, соответствующие выбранным направлениям разработки
Классический подход	Автономность инструментов Четкая функциональность Простота внедрения	Базовые инструменты защиты конечных точек Продвинутые инструменты защиты конечных точек Инструменты сетевого анализа Инструменты анализа и реагирования на события в сетевом трафике
Экосистемный подход	Взаимодополняемость и совместимость инструментов Единый аналитический центр Автоматизированность типовых задач	Инструменты комплексного учета и анализа событий Инструменты комплексного учета и реагирования
Результативный и усиленный результативный подход	Единый автоматизированный центр управления Автоматизированная система обучения угрозам Активный поиск слабых мест систем	Инструменты комплексного учета и анализа событий Инструменты комплексного учета и реагирования Инструменты проактивной защиты

Заключение

В результате проведенного исследования**:**

1. выделены и описаны современные концептуальные подходы к формированию систем кибербезопасности,
2. выделены и описаны современные подходы к разработке структуры систем кибербезопасности,
3. проведена категоризация современных программных инструментов кибербезопасности,
4. сформирована матрица соответствия подходов и инструментов по категориям.

Результаты исследования могут быть применены для формирования и развития комплексных, непротиворечивых стратегий коммерческих компаний в сфере кибербезопасности.

Список литературы

1. Буди Г., Барито М. Р., Аде Г. А. Стратегическое управление кибербезопасностью [Электронный ресурс]//Форсайт. 2023. №3. С. 88-96. URL:

https://cyberleninka.ru/article/n/strategicheskoe-upravlenie-kiberbezopasnostyu (дата обращения: 3 мая 2024).

2. Боброва М. В., Мастилин А. Е. Машинное обучение в кибербезопасности // Научные междисциплинарные исследования. 2021. №2. С. 24-28. URL: https://cyberleninka.ru/article/n/mashinnoe-obuchenie-v-kiberbezopasnosti (дата обращения: 3 мая 2024).
3. Лебедь С. В. Инновационные технологии в сфере кибербезопасности // Современные информационные технологии и ИТ-образование. 2022. №2. С. 383-390. URL: https://cyberleninka.ru/article/n/innovatsionnye-tehnologii-v-sfere-kiberbezopasnosti (дата обращения: 1 мая 2024).
4. Мамонтова С. В. Экономическая и информационная безопасность в условиях цифровой экономики // РСЭУ. 2022. №4 (59). С. 145-153. URL: https://cyberleninka.ru/article/n/ekonomicheskaya-i-informatsionnaya-bezopasnost-v-usloviyah-tsifrovoy-ekonomiki (дата обращения: 2 мая 2024).
5. Мартынюк М. С. Организационно-управленческие механизмы обеспечения кибербезопасности российских компаний // Финансовые рынки и банки. 2023. №6. С. 5-9. URL: https://cyberleninka.ru/article/n/organizatsionno-upravlencheskie-mehanizmy-obespecheniya-kiberbezopasnosti-rossiyskih-kompaniy (дата обращения: 3 мая 2024).
6. Михайлов А. А., Ермаков А. А. Особенности российского рынка информационной безопасности в современных экономических условиях // Московский экономический журнал. 2023. №3. С. 502-511. URL: https://cyberleninka.ru/article/n/osobennosti-rossiyskogo-rynka-informatsionnoy-bezopasnosti-v-sovremennyh-ekonomicheskih-usloviyah (дата обращения: 3 мая 2024).
7. Намиот Д.Е., Ильюшин Е.А., Чижов И.В. Искусственный интеллект и кибербезопасность // International Journal of Open Information Technologies. 2022. №9. С. 135-146. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-kiberbezopasnost (дата обращения: 1 мая 2024).
8. Отузов М., Какаев И., Аннагулыев Д., Атамырадова З. Анализ эффективности существующих методов защиты от киберугроз // Всемирный ученый. 2023. №9. С. 193-196. URL: https://cyberleninka.ru/article/n/analiz-effektivnosti-suschestvuyuschih-metodov-zaschity-ot-kiberugroz (дата обращения: 1 мая 2024).
9. Попов Е. Д. Анализ влияния цифровой трансформации на экономическую безопасность организации//Инновации и инвестиции. 2023. №10. С. 165-168. URL: https://cyberleninka.ru/article/n/analiz-vliyaniya-tsifrovoy-transformatsii-na-ekonomicheskuyu-bezopasnost-organizatsii (дата обращения: 3 мая 2024).
10. Утегенов Н. Б. Рост угроз кибербезопасности // Universum: технические науки. 2023. №7-1 (112). С. 35-39. URL: https://cyberleninka.ru/article/n/rost-ugroz-kiberbezopasnosti (дата обращения: 1 мая 2024).
11. Халин В.Г., Чернова Г.В. Цифровизация и киберриски // Управленческое консультирование. 2023. №7 (175). С. 28-41 URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-i-kiberriski (дата обращения: 3 майя 2024).
12. Хомякова М.И., Пратусевич В.Р., Рыжкова Т.Б. Исследование рынка антивирусных программ в РФ в современных условиях // Инновации и инвестиции. 2022. №9. С. 215-

219 URL: https://cyberleninka.ru/article/n/issledovanie-rynka-antivirusnyh-programm-v-rf-v-sovremennyh-usloviyah (дата обращения: 3 мая 2024).

References

1. Budi G., Barito M. R., Ade G. A. Strategic cybersecurity management [Electronic resource] // Foresight. 2023. No. 3. pp. 88-96. URL: https://cyberleninka.ru/article/n/strategicheskoe-upravlenie-kiberbezopasnostyu (date of reference: May 3, 2024).
2. Bobrova M. V., Mastilin A. E. Machine learning in cybersecurity // Scientific interdisciplinary research. 2021. No.2. pp. 24-28. URL: https://cyberleninka.ru/article/n/mashinnoe-obuchenie-v-kiberbezopasnosti (accessed May 3, 2024).
3. Lebedev S. V. Innovative technologies in the field of cybersecurity // Modern information technologies and IT education. 2022. No.2. pp. 383-390. URL: https://cyberleninka.ru/article/n/innovatsionnye-tehnologii-v-sfere-kiberbezopasnosti (date of reference: May 1, 2024).
4. Mamontova S. V. Economic and information security in the digital economy // RSEU. 2022. No.4 (59). pp. 145-153. URL: https://cyberleninka.ru/article/n/ekonomicheskaya-i-informatsionnaya-bezopasnost-v-usloviyah-tsifrovoy-ekonomiki (accessed May 2, 2024).
5. Martynyuk M. S. Organizational and managerial mechanisms for ensuring cybersecurity of Russian companies // Financial markets and banks. 2023. No.6. pp. 5-9. URL: https://cyberleninka.ru/article/n/organizatsionno-upravlencheskie-mehanizmy-obespecheniya-kiberbezopasnosti-rossiyskih-kompaniy (accessed May 3, 2024).
6. Mikhailov A. A., Ermakov A. A. Features of the Russian information security market in modern economic conditions // Moscow Economic Journal. 2023. No.3. pp. 502-511. URL: https://cyberleninka.ru/article/n/osobennosti-rossiyskogo-rynka-informatsionnoy-bezopasnosti-v-sovremennyh-ekonomicheskih-usloviyah (accessed May 3, 2024).
7. Namiot D.E., Ilyushin E.A., Chizhov I.V. Artificial intelligence and cybersecurity // International Journal of Open Information Technologies. 2022. No.9. pp. 135-146. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-kiberbezopasnost (date of application: May 1, 2024).
8. Otuzov M., Kakaev I., Annagulyev D., Atamyradova Z. Analysis of the effectiveness of existing methods of protection against cyber threats // World Scientist. 2023. No.9. pp. 193-196. URL: https://cyberleninka.ru/article/n/analiz-effektivnosti-suschestvuyuschih-metodov-zaschity-ot-kiberugroz (accessed May 1, 2024).
9. Popov E. D. Analysis of the impact of digital transformation on the economic security of an organization // Innovations and investments. 2023. No.10. pp. 165-168. URL: https://cyberleninka.ru/article/n/analiz-vliyaniya-tsifrovoy-transformatsii-na-ekonomicheskuyu-bezopasnost-organizatsii (date of access: May 3, 2024).
10. Utegenov N. B. The growth of cybersecurity threats // Universum: technical Sciences. 2023. No.7-1 (112). pp. 35-39. URL: https://cyberleninka.ru/article/n/rost-ugroz-kiberbezopasnosti (accessed May 1, 2024).
11. Khalin V.G., Chernova G.V. Digitalization and cyber risks // Managerial consulting. 2023. No.7 (175). pp. 28-41 URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-i-kiberriski (date of reference: May 3, 2024).

12. Khomyakova M.I., Pratusevich V.R., Ryzhkova T.B. Market research of antivirus programs in the Russian Federation in modern conditions // Innovations and investments. 2022. No. 9. pp. 215-219 URL: https://cyberleninka.ru/article/n/issledovanie-rynka-antivirusnyh-programm-v-rf-v-sovremennyh-usloviyah (accessed May 3, 2024).