Оценка процессов ИБ в соответствии с их состоянием

0	Начальный: процесс отсутствует или его элементы выполняются частично
1	Выполняемый: основные элементы выполняются бессистемно. Процесс формально не задокументирован или документирован поверхностно, актуализация документации не выполняется. Эффективность функционирования зависит от индивидуальных знаний и усилий исполнителей
2	Установленный процесс: основные элементы процесса задокументированы и в основном выполняются одинаково для всей организации. Выполняется актуализация документации. Роли и обязанности определены и используются на практике. Процесс автоматизирован с помощью технических решений
3	Управляемый процесс: установленный процесс достигает поставленных результатов и генерирует показатели, на основе которых производится оценка его эффективности и усовершенствования
4	Оптимизированный процесс: высшее руководство принимает участие в анализе недостатков и повышении эффективности процесса. Совершенствование процесса и поддерживаемых технологий проводится регулярно и измеряется

Для оценки зрелости процессов ИБ по разным сферам предприятия, предлагаем использовать методологию для оценки зрелости процессов, разработанную на основе ведущих мировых практик и стандартов информационной безопасности. Для этого была создана референсная модель процессов ИБ по разным сферам предприятия (рисунок).

Были выделены следующие процессы:

− УД – Управление доступом к информационным ресурсам

− УИА – Управление информационными активами

− УПД – управление персональными данными

− УНБИС – Управление настройками безопасности ИС и оборудования

− УИНЦ- Управление инцидентами ИБ

− МБЗКТ – Сетевая безопасность и защита конечных точек

− МПИБ-мониторинг событий ИБ

− УВТС – Управление взаимодействием с третьими сторонами

− ЖБК – Обеспечение безопасности кода

− УВ – управление уязвимостями

Каждый процесс приведенной модели оценивается по пятибалльной шкале в соответствии с состоянием процесса на предприятии, толкование оценки процессов приведено в таблице.

Заключение

В этой статье рассмотрены государственные стандарты информационной безопасности, регламентирующие создание КСЗИ и международные стандарты информационной безопасности, что регламентируют построение СУИБ и определяют подход к построению системы управления кибербезопасностью. Были сравнительно государственные и международные стандарты на их соответствие современным тенденциям кибербезопасности.

Была разработана операционная модель, позволяющая систематизированно проанализировать текущее состояние организации в соответствии с требованиями вышеупомянутых стандартов. Каждый раздел, входящий в операционную модель, был описан и приведен этапы проведения анализа для каждого из разделов. Представлен пример результатов анализа текущего состояния операционной модели предприятия, используя вышеупомянутые этапы и рекомендации.

Список литературы

1. Максимова Е. А. Аксиоматика инфраструктурного деструктивизма субъекта критической информационной инфраструктуры // Информатизация и связь. 2022. № 1. С. 68–74. DOI: 10.34219/2078-8320-2022-13-1-68-74. EDN: ZMOPQB.

2. Роберте Ф. С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам / пер. с англ. М.: Наука, 1986. 496 с.

КИБЕРБЕЗОПАСНОСТЬ. АНАЛИЗ ВИДОВ ЗАЩИТЫ В ИНФОРМАЦИОННОЙ СРЕДЕ

Пелипенко А. П.

ФГБОУ ВО «Мелитопольский государственный университет», Мелитополь, e-mail: elena27712@mail.ru

Научный руководитель: Ступницкий В. С.

Введение

В нынешней цифровой среде обеспечение кибербезопасности приобретает первостепенное значение для устойчивого функционирования любой сферы жизни. Что же такое эта кибербезопасность? Это совокупность технических решений, направленных на защиту сетевых инфраструктур, хранимую информацию, устройств, обеспечение конфиденциальности и целостности. С каждым днём рост кибератак привлекает за собой новые виды угроз, а развитие систем защиты становится критически важным. Только в 2025 году было зарегистрировано более 36 фактов взлома с ущербом от 1 до 223 миллионов (USD). Цели кибератак могут быть разными: от кражи конфиденциальных данных, до нарушения работы систем.

Существует множество причин, по которым кибератаки стали такими частыми в наше время: быстрый рост технологий, развитие искусственного интеллекта, массовая цифровизация рабочих процессов, практически полный перенос хранения данных в виртуальные хранилища и облачные серверы. Эти факторы стимулируют злоумышленников разрабатывать новые и инновационные методы атак для достижения политических или коммерческих целей.

Цель исследования – на основе имеющихся данных сформировать целостную картину понимания о текущем состоянии угроз и найти методы противодействия кибератакам.

Материалы и методы исследования

Для достижения цели было проведено глубокое исследование с использованием отчётов ведущих международных агентств по кибербезопасности, статистические данные о кибератаках, актуальные исследования в области кибербезопасности. В ходе исследования были использованы: системный анализ, контент-анализ, сравнительный анализ.

Результаты исследования и их обсуждение

Количество кибератак стремительно усиливается, при этом большинство атак (70%) нацелены на нарушение работы или получение выкупа путём уничтожения данных. Значительная часть этих атак (44%) включает шифрование информации, 32% приводят к полному выводу из строя инфраструктуры. Злоумышленники, активно применяя ИИ для автоматизации, объединяются в группы и концентрируют свои усилия на промышленных, IT и финансовых организациях. Распространённые методы включают фишинг, социальную инженерию и использование уязвимостей веб-приложений. На рисунке 1 представлены актуальные киберугрозы за 2025 год.

Одним из самых распространённых угроз являются DDoS-атаки. В среднем ежедневно атакуется около 1 466 хостов, а в пиковые дни – до 8 532 хостов за сутки, общее число уникальных атакованных хостов за год превысило 483,9 тысячи, самая продолжительная атака длилась 10 дней, что указывает на растущую сложность и настойчивость злоумышленников.

Для защиты применяются комплексные решения (NGFW, EDR, XDR), SIEM-системы, шифрование, а также предиктивная аналитика и машинное обучение. Важнейшими мерами являются обучение сотрудников, внедрение принципа нулевого доверия, регулярное резервное копирование, постоянный мониторинг угроз и быстрое реагирование на инциденты, с учётом законодательных норм и стандартов кибербезопасности. На рисунке 2 представлены меры защиты от кибератак.

Разберём каждое решение и перспективы.

NGFW – является мощным средством защиты сетевой инфраструктуры, позволяющим выявлять многие современные угрозы. Одни из основных возможностей: контроль приложений, идентификация пользователей и устройств, предотвращение вторжений, песочница для файлов, обмен индикаторами, IPS. При грамотном внедрении NGFW, платформа повышает устойчивость и делает политику прозрачной.

EDR – это экспертная система для обнаружения и реагирования на современные угрозы на конечных устройствах (мобильные устройства, компьютер и т.д.). Включает защиту и сбор данных из любой конечной точки, анализ данных, уведомление о подозрительной активности, сохранение данных. Правильно настроенный EDR даёт возможность обнаруживать атаку на самых ранних этапах и отслеживать всю цепочку продвижения по инфраструктуре.

Следующим шагом в развитии технологий стало решение XDR. Это термин, который обозначает расширенное обнаружение и реагирование в сфере информационной безопасности. Его ценность проявляется в удобстве эксплуатации, повышенным уровнем автоматизации и эффективности поиска угроз и реагирования на них. Последовательно работает так: собирает и нормализует данные, анализирует и сопоставляет данные, содействует управлению инцидентами, помогает предотвратить будущие инциденты. XDR упрощает исследование и реагирование на операции безопасности за счёт объединения инструментов от нескольких поставщиков в единую экономичную платформу XDR. По мере роста внедрения, продолжается расширение возможностей данного решения. Одни из будущих трендов: объединение платформ, ИИ и автоматизация, аналитика поведения пользователей.

SIEM – система, обеспечивающая анализ в реальном времени событий безопасности. Основными задачами являются сбор, обработка и анализ событий безопасности, поступающих в систему из многочисленных источников. Не мало важно обнаружение атак в режиме реального времени и выявление нарушений политик безопасности.

Шифрование – это способ преобразования данных, при котором они не смогут быть прочитаны кем-либо, кроме авторизованных сторон. Шифрование не обходится без криптографического ключа. Криптографический ключ – это уникальный набор символов, используемый для шифрования и дешифрования информации. Существует 2 вида: симметричный, при котором один и тот же ключ используется и для шифрования и для дешифрования. Асимметричный: используется пара разных ключей (открытый и закрытый).

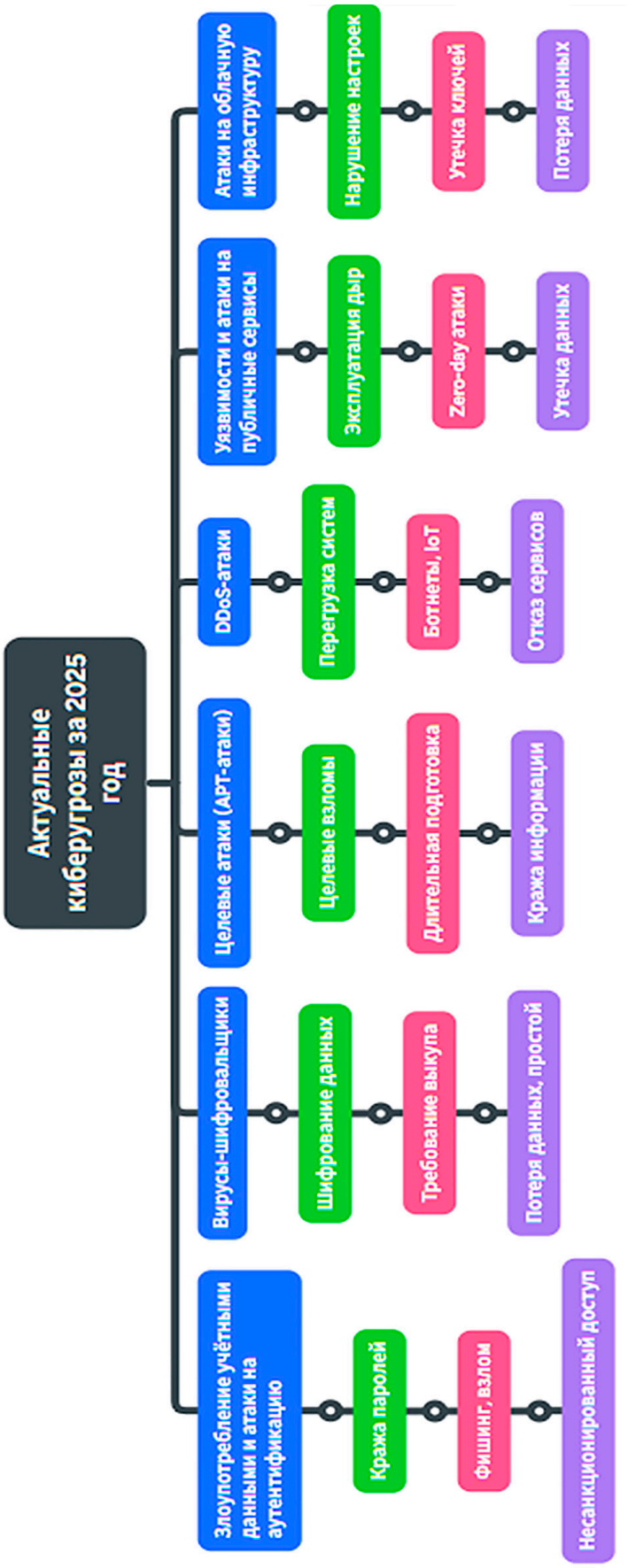

Рис. 1. Актуальные киберугрозы

Рис. 2. Меры защиты от кибератак

Предиктивная аналитика – это автоматизированный способ анализа данных для планирования и прогнозирования событий, который сопровождается алгоритмами машинного обучения и искусственного интеллекта. Используется в разнообразных областях бизнеса: здравоохранении, кредитовании, страховании и государственном секторе. Один из минусов: из-за существования многочисленных факторов, результаты предиктивной аналитики не всегда может быть на 100 процентов достоверными.

Машинное обучение – отрасль искусственного интеллекта, позволяющая системам улучшать свою производительность без необходимости явного программирования. Оно включает в себя несколько этапов: сбор информации, подготовка данных, выбор алгоритма, обучение модели, оценка модели, доработка и внедрение. Машинное обучение открывает новые возможности для всех, кому нужно постоянно иметь дело с большими объёмами информации.

Заключение

Достижение 100 процентов безопасности на данный момент не представляется возможным, но объединив технологические средства, грамотную политику безопасности, осведомлённость пользователей, можно добиться эффективной защиты с области информационной безопасности.

Список источников.

1. Стратегический обзор киберугроз 2025 URL: https://jetcsirt.su/analytics/kurs-na-antikhrupkost-strategicheskiy-obzor-kiberugroz-2025/ (дата обращения: 15.12.2025).

2. Рик Ховард. Кибербезопасность главные принципы. 2024. URL: https://newsletter.radensa.ru/wp-content/uploads/2024/07/Кибербезопасность_главные_принципы_Рик_Ховард_2024.pdf (дата обращения: 15.12.2025).

3. Технология SIEM: полный обзор архитектуры, корреляции событий и интеграции с SOAR. URL: https://serverflow.ru/blog/stati/tekhnologiya-siem-polnyy-obzor-arkhitektury-korrelyatsii-sobytiy-i-integratsii-s-soar/ (дата обращения: 15.12.2025).

4. Объединение силы и интеллекта: XDR как единое решение для надёжной киберзащиты 2023. URL: https://www.securitylab.ru/analytics/544355.php (дата обращения: 17.12.2025).

5. NGFW простыми словами. Как устроены современные межсетевые экраны и чем они отличаются от классических, 2024. URL: https://www.securitylab.ru/analytics/563199.php (дата обращения: 21.12.2025).

СТРАТЕГИЯ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОМ ОТДЕЛЕНИИ

Поздняков И. В., Букреев Д. А.

ФГБОУ ВО «Мелитопольский государственный университет», Мелитополь,
e-mail: dmitriy.bukreev@mel-su.ru

Научный руководитель: Букреев Д.А.

Введение

Современная банковская деятельность в значительной степени опирается на использование информационных технологий, обеспечивающих обработку финансовых операций, хранение персональных данных клиентов и взаимодействие с государственными и межбанковскими информационными системами. В условиях цифровизации финансового сектора банковские отделения становятся не только точками обслуживания клиентов, но и важными элементами распределённой информационной инфраструктуры, от устойчивости и защищённости которых напрямую зависит надёжность функционирования кредитной организации в целом. Рост числа киберинцидентов в финансовой сфере, усложнение методов атак и повышение их целенаправленного характера актуализируют задачу перехода от фрагментарных мер защиты к стратегическому управлению информационной безопасностью. Банковские отделения, несмотря на ограниченные по сравнению с центральными офисами ресурсы, обрабатывают значительные объёмы конфиденциальной информации и нередко становятся уязвимым звеном в общей системе защиты. Это обусловлено сочетанием технических, организационных и человеческих факторов, включая использование автоматизи-