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-

рованных рабочих мест, локальных сетей, периферийного оборудования и удалённых каналов доступа. Особенность обеспечения информационной безопасности в банковском отделении заключается в необходимости сочетать высокие требования к защите информации с непрерывностью бизнес-процессов и удобством обслуживания клиентов. Избыточно жёсткие меры безопасности способны снижать операционную эффективность, тогда как недостаточная защищённость создаёт предпосылки для утечек данных, финансовых потерь и репутационного ущерба. В этой связи особую значимость приобретает разработка стратегии информационной безопасности, ориентированной на системное управление рисками и адаптацию защитных мер к реальным условиям функционирования отделения.

Цель исследования – разработка и обоснование стратегии повышения уровня информационной безопасности в банковском отделении на основе анализа существующих угроз и уязвимостей.

Материал и методы исследования

В рамках исследования рассматривались автоматизированные рабочие места сотрудников, локальная вычислительная сеть отделения, используемое прикладное и системное программное обеспечение, а также регламенты обработки и защиты информации. Эмпирическую базу исследования составили нормативные и методические документы в области информационной безопасности банковской деятельности, требования регуляторов финансового сектора, а также открытые аналитические материалы, отражающие современные тенденции развития угроз и уязвимостей в кредитных организациях. Учитывались особенности функционирования банковского отделения как элемента распределённой инфраструктуры, взаимодействующего с центральными банковскими системами, платёжными шлюзами и внешними сервисами. Методологическая основа исследования базируется на сочетании аналитических и практико-ориентированных методов. В первую очередь применялся структурно-функциональный анализ, позволивший рассмотреть банковское отделение как совокупность взаимосвязанных подсистем – технической, программной, организационной и кадровой. Для оценки актуальных угроз и уязвимостей использовался риск-ориентированный метод, предполагающий идентификацию потенциальных источников угроз, анализ вероятности их реализации и оценку возможного ущерба. Это позволило перейти от формального соответствия требованиям безопасности к осмысленному управлению рисками, что является основой стратегического подхода к защите информации.

Результаты исследования и их обсуждение

Текущее состояние информационной безопасности банковского отделения формируется под воздействием совокупности технических, организационных и человеческих факторов, каждый из которых в отдельности может не представлять критической угрозы, однако в совокупности способен существенно снизить общий уровень защищённости. В условиях распределённой банковской инфраструктуры отделение выступает как автономный, но тесно связанный с центральными системами элемент, что делает его одновременно уязвимым и значимым с точки зрения обеспечения устойчивости всей информационной системы банка.

Особенность анализа информационной безопасности на уровне отделения заключается в необходимости учитывать реальные условия эксплуатации: ограниченные вычислительные ресурсы, высокую нагрузку на персонал, интенсивный поток клиентов и жёсткие требования к непрерывности обслуживания [1]. В таких условиях меры защиты зачастую реализуются фрагментарно и ориентированы преимущественно на выполнение формальных требований, что снижает их эффективность при возникновении нестандартных ситуаций и целевых атак.

1. Организационная составляющая системы информационной безопасности банковского отделения играет ключевую роль, поскольку именно она определяет порядок применения технических средств защиты и поведение персонала в различных ситуациях. Анализ показывает, что в ряде случаев политика информационной безопасности носит декларативный характер и недостаточно адаптирована к условиям конкретного отделения. Регламенты и инструкции по защите информации часто разрабатываются на уровне головного офиса и не учитывают специфику локальных бизнес-процессов. В результате сотрудники воспринимают требования безопасности как формальные ограничения, что приводит к их частичному игнорированию или формальному выполнению. Недостаточная регламентация ответственности и отсутствие чётких процедур реагирования на инциденты дополнительно усиливают риски, связанные с человеческим фактором.

2. Программно-аппаратная инфраструктура банковского отделения, как правило, включает автоматизированные рабочие места сотрудников, локальную вычислительную сеть, серверные компоненты и периферийные устройства. Анализ состояния этих элементов показывает, что основными источниками уязвимостей являются неоднородность используемого оборудования и программного обеспечения, а также несвоевременное обновление средств защиты. В условиях ограниченных ресурсов часть рабочих станций может эксплуатироваться дли-

тельное время без модернизации, что повышает вероятность использования уязвимостей операционных систем и прикладных программ. Средства антивирусной защиты и межсетевые экраны нередко функционируют в стандартных конфигурациях, не адаптированных под конкретные угрозы, характерные для банковского сектора. Это снижает их способность эффективно противодействовать целенаправленным атакам и современным вредоносным программам.

3. Человеческий фактор остаётся одним из наиболее значимых источников рисков информационной безопасности в банковском отделении. Сотрудники ежедневно работают с конфиденциальной информацией и взаимодействуют с клиентами, что создаёт благоприятные условия для реализации методов социальной инженерии. При этом уровень осведомлённости персонала в вопросах информационной безопасности зачастую оказывается недостаточным для своевременного распознавания угроз. Отсутствие регулярного обучения и практических тренингов приводит к тому, что сотрудники не всегда осознают последствия своих действий, связанных с обработкой информации и использованием информационных систем. Использование простых паролей, передача учётных данных, работа с подозрительными электронными сообщениями – все эти факторы повышают вероятность компрометации данных и нарушений безопасности.

В целом анализ текущего состояния информационной безопасности банковского отделения показывает, что существующие меры защиты не всегда образуют единую и согласованную систему. Фрагментарность организационных решений, технические ограничения и влияние человеческого фактора создают предпосылки для возникновения инцидентов безопасности. Это обуславливает необходимость перехода от локальных корректирующих мер к разработке и реализации целостной стратегии повышения информационной безопасности.

Разработка стратегии повышения информационной безопасности банковского отделения должна опираться на результаты комплексного анализа текущего состояния защищённости и учитывать, как внутренние особенности функционирования отделения, так и внешние регуляторные и технологические требования. В отличие от набора разрозненных защитных мер, стратегия предполагает системный и долгосрочный подход, ориентированный на управление рисками, адаптацию к изменяющейся угрозовой обстановке и устойчивое развитие системы безопасности.

Стратегический подход позволяет перейти от реагирования на отдельные инциденты к проактивному управлению информационной безопасностью. В условиях банковской деятельности это особенно важно, поскольку последствия нарушений безопасности выходят за рамки локальных потерь и могут затрагивать финансовую устойчивость, репутацию и доверие клиентов к кредитной организации.

В основе стратегии повышения информационной безопасности банковского отделения лежит ряд базовых принципов, определяющих логику принятия решений и выбор защитных мер:

1. К числу ключевых принципов относится приоритет риск-ориентированного подхода, при котором ресурсы направляются на защиту наиболее критичных активов и процессов. Такой подход позволяет обеспечить рациональное использование средств и избежать избыточных мер, не приносящих существенного повышения уровня защищённости.

2. Не менее важным является принцип согласованности стратегии информационной безопасности с бизнес-целями банковского отделения. Защитные меры не должны препятствовать выполнению основных функций обслуживания клиентов и обработки финансовых операций. Напротив, стратегия должна способствовать повышению устойчивости бизнес-процессов и снижению вероятности их нарушения вследствие инцидентов безопасности [2].

3. Дополнительным принципом выступает адаптивность стратегии, предполагающая её регулярный пересмотр с учётом изменения угроз, технологий и нормативных требований. В условиях быстрого развития цифровых финансовых сервисов статическая модель защиты оказывается неэффективной, что требует постоянного мониторинга и корректировки принятых решений.

Реализация стратегии повышения информационной безопасности в банковском отделении предполагает выделение нескольких ключевых направлений, каждое из которых ориентировано на снижение определённой группы рисков. Одним из таких направлений является совершенствование организационно-управленческой структуры информационной безопасности. Чёткое распределение ролей и ответственности, актуализация внутренних регламентов и формирование процедур реагирования на инциденты создают основу для эффективного применения технических средств защиты.

Важным стратегическим направлением является модернизация программно-аппаратной инфраструктуры с учётом актуальных угроз. Это включает унификацию используемых средств защиты, централизованное управление обновлениями и настройками, а также внедрение механизмов контроля целостности и мониторинга состояния информационных систем. Такой подход позволяет снизить вероятность эксплуатации уязвимостей, связанных с устаревшими или некорректно настроенными компонентами.

Отдельного внимания заслуживает развитие системы управления доступом и аутентификации. В условиях банковского отделения, где сотрудники имеют доступ к различным уровням информа-

ции, стратегически важно обеспечить принцип минимально необходимых привилегий и предотвратить несанкционированное расширение прав доступа [2]. Это снижает риски как внешних атак, так и внутренних нарушений безопасности.

Эффективность стратегии информационной безопасности во многом определяется степенью её интеграции в общую систему управления банковским отделением. Стратегия не должна существовать изолированно в виде формального документа [5], а должна быть встроена в процессы планирования, контроля и оценки деятельности отделения.

Интеграция стратегии предполагает регулярную оценку уровня информационных рисков, использование показателей эффективности защитных мер и проведение внутренних аудитов безопасности. Это позволяет не только выявлять слабые места, но и оценивать результативность реализуемых мероприятий. Важную роль играет также обратная связь от персонала, позволяющая учитывать практические аспекты применения защитных мер и корректировать стратегию с учётом реальных условий эксплуатации.

Таким образом, формирование стратегии повышения информационной безопасности банковского отделения представляет собой многоэтапный процесс, ориентированный на системное управление рисками и устойчивость информационной инфраструктуры [3]. Заложенные в стратегии принципы и направления создают основу для практической реализации конкретных мероприятий, которые рассмотрим более конкретно. В отличие от разрозненных технических решений, практическая реализация стратегии ориентирована на согласованное развитие организационных, технических и кадровых компонентов системы безопасности, что позволяет обеспечить их взаимное усиление и устойчивость к изменяющимся условиям. Практическая ценность стратегии проявляется именно на уровне повседневной деятельности отделения, где защитные меры должны быть встроены в рабочие процессы и восприниматься персоналом как неотъемлемая часть профессиональной деятельности, а не как внешнее ограничение.

Одним из ключевых направлений практической реализации стратегии является модернизация технических и программных средств защиты информации. В условиях банковского отделения приоритет отводится унификации и централизации средств защиты, что позволяет снизить вероятность ошибок конфигурации и упростить администрирование.

1. Практическая реализация данного направления включает внедрение централизованного управления антивирусной защитой и средствами контроля целостности, а также регулярное обновление операционных систем и прикладного программного обеспечения [4]. Особое внимание уделяется защите автоматизированных рабочих мест сотрудников, которые являются основной точкой взаимодействия с банковскими информационными системами и, одновременно, одним из наиболее уязвимых элементов инфраструктуры.

2. Дополнительно в рамках стратегии предусматривается усиление сетевой защиты, включая актуализацию правил межсетевого экранирования, контроль удалённого доступа и мониторинг сетевого трафика. Такие меры позволяют своевременно выявлять аномальную активность и предотвращать развитие инцидентов безопасности на ранней стадии.

3. Организационные меры играют системообразующую роль в реализации стратегии информационной безопасности. Даже наиболее совершенные технические решения теряют эффективность при отсутствии чётко выстроенных регламентов и осознанного участия персонала. В этой связи стратегия предусматривает актуализацию внутренних нормативных документов, регламентирующих порядок работы с информацией, использование средств защиты и реагирование на инциденты.

Практическая реализация организационных мер включает проведение регулярных инструктажей и обучающих мероприятий для сотрудников банковского отделения. Обучение ориентировано не только на формальное ознакомление с требованиями безопасности, но и на формирование понимания возможных последствий нарушений и роли каждого сотрудника в обеспечении защиты информации. Особое внимание уделяется управлению доступом и ответственности персонала. Чёткое разграничение прав, фиксация действий пользователей и контроль соблюдения регламентов позволяют снизить риски, связанные с внутренними нарушениями и человеческим фактором. В рамках стратегии также предусматривается формирование культуры информационной безопасности, при которой соблюдение требований защиты воспринимается как профессиональный стандарт.

Оценка эффективности реализуемых мер осуществляется на основе анализа инцидентов безопасности, результатов внутренних проверок и показателей информационных рисков. Такой подход позволяет выявлять слабые места и корректировать стратегию без ожидания серьёзных нарушений. В условиях банковского отделения особую значимость приобретает оперативность такой оценки, поскольку задержки в принятии решений могут привести к существенным финансовым и репутационным потерям.

Адаптация стратегии предполагает не только обновление технических средств защиты, но и пересмотр организационных подходов, программ обучения персонала и механизмов контроля. Это обеспечивает гибкость системы информационной безопасности и её соответствие актуальным условиям функционирования банковского отделения.

Заключение

Анализ текущего состояния информационной безопасности выявил, что основными источниками рисков на уровне банковского отделения являются фрагментарность организационных решений, неоднородность программно-аппаратной инфраструктуры и влияние человеческого фактора. Формальное выполнение требований безопасности без их адаптации к реальным условиям функционирования отделения снижает эффективность защитных мер и не позволяет своевременно реагировать на изменение угрозовой обстановки. Сформированная стратегия повышения уровня защищённости ориентирована на согласование мер безопасности с бизнес-процессами банковского отделения, обеспечение адаптивности системы защиты и её интеграцию в процессы управления и контроля. Такой подход позволяет не только снизить вероятность реализации актуальных угроз, но и повысить устойчивость информационной инфраструктуры в долгосрочной перспективе. Модернизация средств защиты, развитие системы управления доступом, повышение уровня осведомлённости персонала и регулярная оценка эффективности принятых решений позволяют сформировать целостную и управляемую систему информационной безопасности на уровне банковского отделения. Таким образом, стратегия повышения информационной безопасности банковского отделения должна рассматриваться как непрерывный процесс, направленный на управление рисками, адаптацию к изменяющимся условиям и поддержание доверия клиентов.

Список литературы

1. Столлингс У. Криптография и защита сетей: принципы и практика. М.: Вильямс, 2020.
2. Шнайер Б. Прикладная криптография. М.: Диалектика, 2019.
3. Таненбаум Э., Уэзеролл Д. Компьютерные сети. СПб.: Питер, 2021.
4. Pfleeger C., Pfleeger S., Margulies J. Security in Computing. Pearson, 2020.
5. ISO/IEC 27001:2022. Information Security Management Systems – Requirements.

МОДЕЛЬ ЯСТРЕБ-ГОЛУБЬ ДЛЯ АНАЛИЗА АГРЕССИВНОГО И ДРУЖЕЛЮБНОГО ВЕБ-ИНТЕРФЕЙСА

Попов Т. И., Покуса Т. В.

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

Научный руководитель: Покуса Т. В.

Введение

Современный интернет имеет крайне широкий спектр выбора для пользователей среди сайтов предоставляющие услуги. Регулярно случаются инциденты, когда интернет-пользователи могут столкнуться с мошенническим сайтом, или как минимум – с сайтом использующие человеческие качества пользователя для того, чтобы повысить конверсию своей площадки. Такой подход зачастую агрессивен с точки зрения дизайна и маркетинга, с другой стороны существуют сайты с повышенной прозрачностью и вызовом доверия у пользователей, но они парадоксально имеют куда меньший охват пользователей, чем сайты с агрессивным подходом. С точки зрения теории игр, эти две категории сайтов можно поделить на две группы: «Ястребы» и «Голуби». Согласно математической модели «Ястребы и голуби», её смысл состоит в описывании конкурентных отношений в некоторой популяции животных и выработки оптимальной эволюционной стратегии. Данная модель будет адаптирована для экосистем рынка веб-сайтов: «Ястреб» – сайты использующие методы скрытого воздействия в дизайне и громкую рекламу, «Голуби» – сайты менее заметные, чем «ястребы» из-за меньшей рекламной политики и имеющие большую степень честности по отношению к покупателям. Используя вышеуказанную модель из теории игр, в данной научной работе будет исследоваться потенциальна наиболее выгодная модель для рынка и при каких условиях рынок может достичь равновесия в конкуренции «голубей» и «ястребов». Практическая значимость состоит в том, что формализация конфликта даёт чёткие критерии, по которым пользователи распознают манипулятивные сайты. Модель позволяет владельцам площадок и аналитикам проверить, насколько выгодна та или иная стратегия при сложившихся условиях рынка, а также определить долю «ястребов» и «голубей», при которой рынок переходит в устойчивое состояние.

Цель исследования – нахождение точки равновесия в интернет-рынке для сайтов из групп «ястребов» и «голубей». Вычисление наиболее оптимальной стратегии поведения для веб-сайтов. Найти способ распознавать сайты использующие манипуляции.

Материалы и методы исследования

В работе используется метод из теории игр «Ястреб и голубь». Джон Мейнард Смит описал ситуацию, в которой животные выбирают: уступить или драться. Это вариант игры «Струсил – проиграл». В споре за добычу оба соперника обычно проявляют агрессию и стремятся ранить друг друга. Непосредственно перед схваткой каждый решает: отступить, оставив добычу, но оставившись живым (голубь), или продолжать бой до конца, рискуя погибнуть (ястреб). Предположим, в популяции, где все ведут себя как голуби, появляется небольшая партия ястребов. Сначала доля ястребов увеличивает-