

34. ИНСТРУМЕНТЫ, МЕХАНИЗМЫ И ПРАКТИКА ПРИМЕНЕНИЯ КИБЕРБЕЗОПАСНОСТИ В ЭЛЕКТРОННОМ БИЗНЕСЕ В БЕЛАРУСИ

Севрюков С.И., Горбачев А.К., Макаревич Д.Н.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Ермакова Е.В. – канд. экон. наук

В работе рассматриваются практические аспекты обеспечения кибербезопасности в электронном бизнесе Беларуси. Особое внимание уделено механизмам защиты, включая требования законодательства, создание центров кибербезопасности, защиту персональных данных и реагирование на инциденты, а также роли государственных структур и международных стандартов в данной области.

Цифровизация экономики значительно увеличивает риски для электронного бизнеса, включая утечку данных, атаки на информационные системы и угрозы безопасности цифровых сервисов. Эффективная кибербезопасность становится необходимостью для успешной работы и развития цифровых компаний. В Республике Беларусь созданы правовые и организационные условия для внедрения киберзащиты в электронный бизнес, и в этом контексте важным становится понимание того, как эти меры реализуются на практике.

Киберугрозы могут проявляться в самых разных формах, начиная от фишинга и заканчивая более сложными атаками, такими как DDoS-атаки, вирусные атаки или утечка персональных данных. Например, фишинг-атаки, направленные на пользователей интернет-магазинов, могут привести к краже их личных данных и банковских реквизитов. Белорусские компании сталкивались с масштабной утечкой данных, что привело к значительному финансовому ущербу и потере доверия со стороны клиентов.

Инциденты с киберугрозами могут иметь долгосрочные последствия для бизнеса. Репутационные потери часто оказываются более серьезными, чем прямые финансовые. Например, случаи с утечками данных или атакой на веб-сайт могут привести к падению пользовательской активности, снижению числа заказов и росту числа возвратов товаров, что в свою очередь приведёт к потерям.

Одним из примеров практического применения кибербезопасности в Беларуси является внедрение системы мониторинга трафика для выявления подозрительных действий. Например, крупные белорусские торговые платформы используют систему обнаружения аномальной активности в реальном времени, что позволяет оперативно блокировать подозрительные транзакции и минимизировать потери.

Согласно законодательству, компании, работающие в сфере электронной коммерции, обязаны создать или заключить договора с центрами кибербезопасности для защиты своих информационных систем. Одним из важнейших требований является наличие системы для оперативного реагирования на инциденты. В 2023 году многие белорусские компании начали активно внедрять такие системы для мониторинга угроз и защиты от кибератак, что позволяет им оперативно реагировать на возникающие угрозы [1].

Одним из ярких примеров является разработка и внедрение интегрированных систем реагирования на инциденты, таких как СОК (Security Operations Center). В Беларуси крупные интернет-магазины внедрили СОК-системы, которые позволяют в реальном времени отслеживать потенциальные угрозы, автоматически блокировать подозрительные действия и минимизировать последствия инцидентов. К примеру, такие системы могут автоматически блокировать IP-адреса, с которых поступают DDoS-атаки, или запускать механизмы защиты при попытке несанкционированного доступа.

Один из примеров защиты персональных данных в электронном бизнесе — внедрение системы шифрования данных на этапе передачи и хранения. Для защиты данных клиентов, интернет-магазины используют SSL-сертификаты для безопасной передачи информации. Также активно применяется двухфакторная аутентификация для доступа к аккаунтам пользователей.

Государственные структуры, такие как Оперативно-аналитический центр (ОАЦ) и Национальный центр обеспечения кибербезопасности, активно контролируют и координируют мероприятия в сфере киберзащиты. ОАЦ разрабатывает стратегии и регламенты по защите информационных систем, а Национальный центр обеспечивает мониторинг угроз и их анализ.

Для проверки выполнения требований в сфере кибербезопасности Национальный центр проводит регулярные аудиты в компаниях [2]. В ходе аудита специалисты проверяют не только техническую защищенность, но и соответствие внутренней документации нормам законодательства.

Национальный центр и ОАЦ создают и поддерживают системы для постоянного мониторинга угроз в национальном сегменте Интернета. Практически это проявляется в регулярных отчетах, а также в системе, где компании могут обмениваться информацией о текущих угрозах и предпринимаемых мерах защиты.

Внутренние меры защиты включают регулярные аудиты и тестирование на уязвимости. В Беларуси многие компании, особенно крупные игроки в сфере электронной коммерции, проводят как внутренние, так и внешние аудиты безопасности. Одним из примеров является регулярное использование тестов на проникновение (pen-test) для оценки уязвимостей в системе. Такие тесты выявляют слабые места, которые могут быть использованы злоумышленниками.

Компании в Беларуси активно разрабатывают внутреннюю документацию по безопасности, которая включает политики по защите информации, регламенты по реагированию на инциденты и другие нормативные документы. Важной частью этой документации являются инструкции по безопасному использованию корпоративных систем, а также правила для сотрудников по защите конфиденциальных данных.

Важно, чтобы информация о киберинцидентах хранилась не менее одного года. Это позволяет не только соответствовать законодательным требованиям, но и разрабатывать более эффективные методы защиты. Многие белорусские компании создают базы данных инцидентов для анализа и прогнозирования новых угроз. Примером является использование этих данных для тренировки машинного обучения с целью прогнозирования и предотвращения будущих атак.

Важной частью стратегии кибербезопасности является развитие кадров. Многие белорусские компании создают специализированные команды информационной безопасности, которые занимаются

мониторингом угроз, реагированием на инциденты и анализом рисков. Эти команды также работают с внешними консультантами и экспертами, что позволяет повышать квалификацию и улучшать защиту.

Белорусские университеты и институты предлагают образовательные программы, направленные на подготовку специалистов по кибербезопасности. Компании активно сотрудничают с образовательными учреждениями, предоставляя студентам возможность проходить стажировки и практику. Примером является программа в Белорусском государственном университете информатики и радиоэлектроники, которая подготовила множество специалистов в области ИБ.

Международный стандарт ISO/IEC 27001 является основой для разработки эффективной системы управления информационной безопасностью [3]. Компании в Беларуси активно используют этот стандарт для создания и внедрения процедур, обеспечивающих безопасность информации. Внедрение ISO/IEC 27001 помогает не только соответствовать международным требованиям, но и улучшать внутренние процессы управления рисками.

Белорусские компании активно перенимают международный опыт, участвуя в международных конференциях, обмениваясь знаниями с зарубежными коллегами и следуя международным стандартам [4]. Это помогает улучшать качество защиты и применять лучшие мировые практики в области кибербезопасности.

Практическое применение кибербезопасности в Беларуси активно развивается. Компании внедряют новые технологические и организационные меры, соответствующие требованиям законодательства, для минимизации рисков и защиты своих цифровых активов. Государственные структуры играют важную роль в координации усилий и контроле за соблюдением требований. В результате, электронный бизнес в Беларуси становится более устойчивым к киберугрозам, что способствует его успешному и безопасному развитию в условиях цифровизации экономики.

Список использованных источников:

1. О кибербезопасности : Указ Президента Республики Беларусь от 14 февр. 2023 г. № 40. – Минск, 2023.
2. Губаревич И. П. Проблемы и перспективы развития законодательства в области кибербезопасности в Республике Беларусь // Вопросы информационной безопасности. – 2022. – № 3. – С. 45-59.
3. ISO/IEC 27001:2022 – Information security management systems. – Женева: Международная организация по стандартизации, 2022. – 72 с.
4. Петрухин В. В., Сидоров И. А. Национальные стратегии кибербезопасности: международный опыт и его адаптация для Республики Беларусь // Журнал международного права. – 2023. – № 2. – С. 89-103.