Павлова Кристина Юрьевна
студентка
Хайруллина Айгуль Айратовна
студентка
Юсупова Агния Сергеевна
канд. социол. наук, доцент

ФГБОУ ВО «Казанский государственный энергетический университет»
г. Казань, Республика Татарстан

КИБЕРБЕЗОПАСНОСТЬ КАК ПРИОРИТЕТНЫЙ РИСК ДЛЯ БИЗНЕСА

Аннотация*: в статье рассматривается кибербезопасность как приоритетный риск для бизнеса в условиях стремительного развития информационных технологий и роста числа киберугроз. Авторы предлагают комплексный подход к управлению киберрисками, включая разработку политики безопасности, внедрение технических мер защиты, обучение сотрудников, создание системы реагирования на инциденты и другие меры.*

Ключевые слова*: кибербезопасность, риск-менеджмент, кибератаки, угрозы для бизнеса, управление рисками, защита данных, информационные технологии.*

В эпоху стремительной цифровизации, когда бизнес все больше интегрируется с информационными технологиями, кибербезопасность стала не просто технической проблемой, а стратегическим вопросом, от которого зависит выживание и процветание любой организации.

Актуальность темы «Кибербезопасность как приоритетный риск для бизнеса» обусловлена растущими угрозами, финансовыми последствиями, репутационными рисками и необходимостью соблюдения законодательства.

Кибербезопасность – это комплекс мер, направленный на защиту информационных систем, данных, сетей и устройств от несанкционированного доступа, использования, раскрытия, изменения или уничтожения. В современном мире,

где бизнес все больше зависит от цифровых данных и онлайн-сервисов, отсутствие надлежащего уровня кибербезопасности создает серьезные риски, которые могут привести к катастрофическим последствиям [3].

Основные типы киберугроз и их влияние на организацию.

1. Фишинг. Фишинг является значительной угрозой, представляющей собой метод обмана, при котором злоумышленники используют поддельные электронные письма или веб-сайты для получения конфиденциальной информации. Данная техника нацелена на манипуляцию пользователями, заставляя их раскрывать пароли или данные банковских карт. Фишинг не только приводит к утечкам данных, но также может повлечь за собой значительные репутационные и финансовые убытки для организации. Для бизнеса это создает необходимость в постоянном обучении сотрудников и внедрении технических решений, таких как системы фильтрации электронной почты [4].

2. DDoS-атаки. Кибератаки на уровне сети, известные как DDoS-атаки (Distributed Denial of Service), также представляют собой серьезную угрозу. Такие атаки стремятся перегрузить сервер или сеть, отправляя на них огромные объемы трафика, что делает их недоступными для пользователей. Это может привести к простою сервисов, что, в свою очередь, вызывает убытки и снижение доверия со стороны клиентов. Установление систем защиты, таких как балансировщики нагрузки и решения для распределения трафика, становится необходимым условием для обеспечения непрерывности бизнеса.

3. Внутренние угрозы. Внутренние киберугрозы могут исходить от сотрудников организаций. Это может быть как умышленное действие, связанное с кражей информации, так и случайная ошибка, например, установка вредоносного ПО на рабочем компьютере. Проведение регулярных аудитов безопасности, внедрение политик контроля доступа и организаций программ обучения по безопасности становятся важными мерами для снижения этих рисков.

Кибератаки могут привести к серьёзным последствиям для бизнеса, таким как финансовые потери, которые включают в себя кражу денежных средств, вы-

могательство, потерю прибыли из-за простоя бизнеса и убытки от репутационных потерь, репутационный ущерб, связанный с потерей доверия клиентов, партнёров и инвесторов, а также негативным влиянием на бренд, нарушение деятельности, включающее простой бизнес-процессов, перебои в работе IT-систем и потерю доступа к данным и юридические проблемы, которые связаны с ответственностью перед регуляторами за нарушение законодательства о защите данных и исками от пострадавших клиентов. Примеры реальных случаев кибератак и их последствий для бизнеса включают Marriott (2018) и Target (2013). В первом случае хакеры получили доступ к данным 500 миллионов гостей, что привело к штрафам на сумму 124 миллионов долларов и потере доверия клиентов. Во втором случае хакеры похитили данные кредитных карт 40 миллионов клиентов, что вызвало финансовые потери на сумму 185 миллионов долларов и потерю доверия клиентов. Данные случаи демонстрируют реальные последствия кибератак для бизнеса, подчеркивая важность эффективного управления кибербезопасностью и риск-менеджмента [2].

Времена простых вирусов, распространяемых по электронной почте, давно прошли. Современные атаки стали более изощренными, используя уязвимости в программном обеспечении, социальную инженерию и даже искусственный интеллект. Например, в 2017 году атака WannaCry парализовала работу больниц и предприятий по всему миру, вызвав массовые сбои и финансовые потери. Хакеры использовали эксплойт для уязвимости в операционной системе Windows. Вредоносные программы стали более сложными, применяя методы обфускации (запутывания кода), полиморфизма (изменения формы) и маскировки, чтобы избежать обнаружения антивирусными программами. Так, в 2017 году вирус NotPetya нанес ущерб компаниям по всему миру, шифруя файлы и требуя выкуп. Вирус использовал уязвимость в программном обеспечении, быстро распространился по сети, а его шифрование было очень сложным.

Искусственный интеллект стал мощным оружием в руках киберпреступников. Он используется для автоматизации атак, поиска уязвимостей, создания фишинговых писем и генерации вредоносного кода. ИИ позволяет таргетировать

атаки на определенные группы людей или компании, используя информацию из социальных сетей и других источников. Искусственный интеллект также используется для создания поддельных видео и аудио материалов, а также для имитации личности с целью обмана. В результате, киберпреступники могут создавать реалистичные фальсификаци, которые трудно отличить от настоящих. В 2022 году был зафиксирован случай использования deepfake-технологий для кражи денег с банковских счетов. Хакеры использовали глубокое обучение, чтобы создать голос, идентичный голосу клиента, и обмануть оператора банка. Новыми угрозами стали атаки на интернет-вещей (IoT), эксплуатирующие уязвимости в бытовых устройствах, интеллектуальных системах и промышленном оборудовании. Киберпреступники также атакуют поставщиков, чтобы получить доступ к информации о компаниях-клиентах, устраивая масштабные атаки на многих компаниях одновременно. В 2020 году атака на Mirai botnet затронула миллионы IoT-устройств, что привело к отказу в обслуживании многих сайтов. Атаку осуществили с помощью ботнета, состоящего из зараженных IoT-устройств, таких как камеры видеонаблюдения и маршрутизаторы. Искусственный интеллект создает новые вызовы для систем кибербезопасности, требуя новых подходов и технологий. Необходимо развивать системы защиты, которые могут обнаруживать и блокировать атаки, использующие ИИ, а также обучать специалистов по кибербезопасности работать с ИИ-инструментами для предотвращения кибератак.

Для защиты информации, систем и бизнеса необходимо выстроить надежную систему безопасности, основанную на комплексных стратегиях и современных инструментах. Ключевым элементом эффективной кибербезопасности являются основные принципы защиты, которые должны лежать в основе любой стратегии. К ним относятся: конфиденциальность, целостность и доступность данных. Конфиденциальность гарантирует, что доступ к информации имеют только авторизованные лица. Целостность обеспечивает сохранность информации от несанкционированных изменений, а доступность позволяет получить доступ к информации в любое время [1].

Инструменты и технологии кибербезопасности играют решающую роль в реализации этих принципов. Современные антивирусные программы, системы обнаружения вторжений, фаерволы и другие инструменты защищают системы от внешних угроз. Для повышения эффективности используются технологии искусственного интеллекта, машинного обучения и аналитики больших данных, позволяющие обнаруживать аномалии и угрозы, а также прогнозировать потенциальные атаки.

Обучение сотрудников является неотъемлемой частью стратегии кибербезопасности. Сознательность сотрудников является ключевым фактором в предотвращении кибератак, основанных на социальной инженерии. Регулярные тренинги, информирование о современных угрозах и правилах безопасного пользования цифровыми ресурсами повышают уровень защищенности компании. Законодательная база также играет важную роль в обеспечении кибербезопасности. Законы и регламенты, регулирующие сбор, хранение и обработку данных, а также ответственность за киберпреступления, создают правовые основы для защиты цифровой инфраструктуры. Важно следить за изменениями в законодательстве и адаптировать свою практику кибербезопасности к новым требованиям. Кибербезопасность не является статичным состоянием, а требует постоянного развития и совершенствования [5].

В заключение, эффективная кибербезопасность требует комплексного подхода, основанного на прочных принципах защиты, современных инструментах и технологиях, сознательности сотрудников и прочной правовой основе. Постоянное развитие и адаптация к меняющимся угрозам являются ключевыми факторами для поддержания высокого уровня безопасности в цифровом мире. Однако важно помнить, что кибербезопасность – это непрерывный процесс, требующий постоянного внимания и усилий. Только совместными усилиями бизнеса, правительств и специалистов по кибербезопасности можно создать надёжную защиту от киберпреступности и обеспечить безопасность информации, систем и бизнеса в целом. Для достижения максимальной эффективности необходимо также учитывать ин-

дивидуальные особенности каждой организации и отрасли, в которой она работает. Это поможет адаптировать стратегии кибербезопасности под конкретные нужды и требования, обеспечивая тем самым более высокий уровень защиты.

Список литературы

1. Казарян К.К. Управление рисками кибербезопасности / К.К. Казарян // StudNet. – 2022. – №1 [Электронный ресурс]. – Режим доступа: https://clck.ru/3FHPdD (дата обращения: 10.12.2024). – EDN GDVCBT

2. Сухоруков М. Как обеспечить кибербезопасность своего бизнеса в 2024 году / М. Сухоруков [Электронный ресурс]. – Режим доступа: https://clck.ru/3FHPhK (дата обращения: 10.12.2024).

3. Крюков А. Что такое кибербезопасность / А. Крюков [Электронный ресурс]. – Режим доступа: https://clck.ru/3FHPjC (дата обращения: 10.12.2024).

4. Защита малого бизнеса от киберугроз [Электронный ресурс]. – Режим доступа: https://clck.ru/3FHPkQ (дата обращения: 10.12.2024).

5. Зараев А.В. Роль информационных технологи в управлении на предприятии / А.В. Зараев, Р.А. Тимофеев // Формирование конкурентной среды, конкурентоспособность и стратегическое управление предприятиями, организациями и регионами: сборник статей VIII Международной научно-практической конференции. – Пенза, 2023. – С. 123–126. – EDN WSJZSY