

Кибербезопасность в современном бизнесе

Лукьянова Наталья Николаевна

Приамурский государственный университет имени Шолом-Алейхема

Студент

Аннотация

Цель настоящего исследования – анализ текущего состояния и проблемы цифровой составляющей экономической безопасности современной экономики – кибербезопасности предприятия. В основе лежит метод теоретического анализа литературы по исследуемой проблеме и нормативно-правовой базы. Развитие цифровизации финансовых и производственных процессов вызывает рост кибератак на предприятия всех форм собственности, которые способны нанести значительный ущерб всем видам активов и бизнес-процессам предприятия.

Ключевые слова: кибербезопасность, информационная безопасность, экономическая безопасность, налоговая безопасность.

Cybersecurity in modern business

Lukyanova Natalia Nikolaevna

Sholom-Aleichem Priamursky State University

Student

Abstract

The purpose of this study is to analyze the current state and problems of the digital component of economic security of the modern economy - cybersecurity of the enterprise. It is based on the method of theoretical analysis of literature on the problem under study and the regulatory framework. The development of digitalization of financial and production processes causes an increase in cyberattacks on enterprises of all forms of ownership, which can cause significant damage to all types of assets and business processes of the enterprise.

Keywords: cybersecurity, information security, economic security, tax security.

Актуальность темы

Цифровая трансформация дает компаниям большие перспективы развития: расширение возможностей, обеспечение значительного экономического и социального преимущества. Однако вместе с широкими возможностями, появляется проблема информационной безопасности и конфиденциальности. Несанкционированный доступ в информационные системы предприятия может нанести ущерб репутации бренда, привести к серьезным финансовым потерям, в том числе к нормативно-правовым издержкам [Ошибка! Источник ссылки не найден.].

Несмотря на доказанную полезность искусственного интеллекта, не следует игнорировать факт, что технологии искусственного интеллекта и их применение могут подвергнуть организации новым, а иногда и непредсказуемым, угрозам и открыть новые возможности для злоумышленников [2].

Кибератаки способны нанести значительный ущерб вашим данным и активам, привести к финансовым потерям. Кроме того, злоумышленники могут получить доступ в корпоративную сеть и использовать в преступных целях следующую информацию:

- списки клиентов;
- данные банковских карт клиентов;
- структуры ценообразования;
- документация по разработке продуктов;
- планы развития бизнеса;
- описания производственных процессов;
- другие виды интеллектуальной собственности.

Таким образом, кибератаки ставят под угрозу не только саму компанию. Скомпрометированная сеть может служить инструментом доступа в сети других компаний, связанных общими цепочками поставок.

Обзор исследований

Проблемы цифровой экономической безопасности рассмотрены в научных трудах отечественных и зарубежных авторов: Н. Лопатова [1], А.Б. Менисов [2], Г.Ф. Багдасарян [3], А.В. Мазеин [4], С.О. Кузнецова, А.Р. Маргамов и др. В современных условиях цифровизация экономики происходит в очень быстром темпе, в связи с чем модели и подходы, предлагаемые авторами, могут быть дополнены и расширены, в том числе современными статистическими данными, с целью максимального обеспечения информационной безопасности предприятия.

Цель исследования

Цель исследования заключается в изучении негативного влияния кибератак на предприятия, прогнозировании их дальнейшего роста и влияния на бизнес.

Методы и материалы

Методологическую основу исследования составили сбор первичного анализа и изложения информации, метод теоретического анализа литературы и нормативно-правовой базы по исследуемой проблеме, системный подход и аналитика, сравнение, метод экспертных оценок.

Результаты и обсуждения

Кибербезопасность — это комплекс технологических и организационных мер, направленных на защиту информационных активов компании от внешних и внутренних угроз. В малом и среднем бизнесе такие активы включают в себя не только финансовую информацию, но и данные клиентов, контракты, маркетинговые планы и логистические цепочки.

Киберугрозы представляют проблему не только для крупных корпораций и правительств, но и для небольших компаний. Исследования показывают, что малый бизнес особенно сильно подвержен кибератакам, во многом из-за того, что не обладает ресурсами для эффективной защиты [3]. Около 60% малых компаний прекращают свою деятельность в течение шести месяцев после того, как становятся жертвами утечки данных или кибератак.

Целью кибератаки в основном является доступ, уничтожение и изменение конфиденциальной информации, которая включает финансовые активы, финансовую и коммерческую информацию, пароли и многое другое от организаций или предприятий.

По прогнозам ведущего мирового исследователя в мире кибербезопасности Cybersecurity Ventures, опубликованным в журнале о киберпреступности Cybercrime Magazine, если рассматривать киберпреступность как отдельную страну, ожидается, что в 2024 году она нанесёт ущерб на сумму \$9,5 триллиона долларов США по всему миру и станет третьей по величине экономикой в мире после США и Китая [4].

Киберпреступность стала одной из наиболее актуальных проблем современного мира. За последние 5 лет число противоправных деяний в киберпространстве России увеличилось более чем вдвое. Сегодня их доля в общем массиве остается значительной и составляет около 40 процентов. То есть почти каждое второе преступление. А по тяжким и особо тяжким составам этот показатель уже приблизился к 60 процентам. Пострадавшими от незаконных действий в цифровой сфере становятся и физические, и юридические лица, в том числе государственные структуры. Наносится существенный вред экономике и имущественным правам граждан [5].

Еще большее значение кибербезопасность приобретает в условиях повсеместного перехода на удаленную работу. Многие небольшие компании используют незащищенные облачные технологии и инструменты для проведения онлайн-собраний, доступа к учетным программам, рассылки рекламы, закупок и продаж, взаимодействия с клиентами и поставщиками и проведения банковских операций.

С появлением новых технологий и развитием Интернета можно получить доступ к цифровой информации из любой точки мира. Вместе с тем с развитием более совершенных методов обмена информацией (облачных хранилищ и мобильных устройств) преступники стали использовать новые методы для хищения цифровых активов [6].

С развитием дистанционных способов подачи отчетности и отправки банковских документов появляется еще ряд угроз, не связанных с киберпреступностью, но непосредственно влияющий на финансовую и налоговую безопасность предприятия. В частности, обработка и хранение персональных данных работников, потенциальных работников и членов их семей, является предметом особой защиты со стороны государства и подпадает под действие Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" [7]. Работодатели, обрабатывающие такие данные, становятся операторами персональных данных, о чем соответствующие

записи вносятся в государственный реестр. Нарушение порядка обработки и хранения персональных данных контролируется Федеральной службой по надзору в сфере связи, информационных технологий массовых коммуникаций (Роскомнадзор). Штрафы за нарушение довольно внушительные: от увольнения работника, допустившего утечку персональных данных и компенсации работодателем ущерба пострадавшему работнику до штрафов, максимальный из которых составляет 18 млн. руб. Назначение такого штрафа может нанести непоправимый ущерб предприятию.

Еще один аспект цифровой безопасности, на который некоторые предприятия мало обращают внимания, считая его незначительным. Это так называемый «цифровой след», который предприятие оставляет ежедневно в процессе своей деятельности. Отправка отчетов в контролирующие органы, использование интернет-банкинга, сайт со сведениями об организации дают очень большой спектр информации заинтересованным лицам. В частности, налоговым органам. Зачастую собственник разделяет направления бизнеса, диверсифицируя его по разным признакам: территориальный, по специфике деятельности и т.п. Налоговые органы, имея фискальную функцию, в подобных случаях пытаются обвинить предприятие в налоговом дроблении и незаконной оптимизации налогов. Подобные претензии контролеров рассматриваются в судебном порядке и, в случае достаточности доказательств (среди которых и есть отправка отчетности и вход в онлайн-банк с одного IP-адреса), предприятие ожидает огромное доначисление налогов, штрафы и пени, которые зачастую ставят под угрозу само существование компании.

По информации пресс-службы депутата Государственной Думы РФ Антона Немкина со ссылкой на Генпрокуратуру РФ, доля киберпреступлений среди всех видов регистрируемых в России преступлений за последний год увеличилась с 31,8% до 38%. При этом относительно уровня 2023 года их массив возрос на 17,4% (до 240,9 тыс.).

Прежде всего, это касается преступлений, связанных с несанкционированным доступом к информсистемам. Например, только в период с декабря 2023 по февраль 2024 года в «Лаборатории Касперского» зафиксировали шестикратный рост DDoS-атак по сравнению со значением 2022–2023 года. Очевидно, что в дальнейшем структура ИТ-преступлений будет изменяться и расширяться.

Поскольку на карту поставлены финансовая безопасность и будущее бизнеса, организациям любого размера крайне важно понимать возможные проявления информационных угроз.

Кибератаки становятся все более изощренными, и малый бизнес — удобная цель для злоумышленников, так как компании этого сектора часто экономят на защите или полагаются на устаревшие решения. Рассмотрим возможные атаки, негативно влияющие на информационную безопасность предприятия.

Фишинг. Фишинговые атаки с каждым годом становятся все сложнее. Это уже не просто письма с подозрительными ссылками, которые можно распознать по плохой орфографии. Теперь злоумышленники имитируют письма от известных российских банков или операторов связи, что делает их особенно опасными.

Вредоносное программное обеспечение. Распространение вредоносного программного обеспечения может происходить через инфицированные веб-сайты, USB-устройства или даже поддельные обновления программ.

DDoS-атаки. DDoS-атаки могут привести к длительной недоступности онлайн-ресурсов, что особенно критично для интернет-магазинов и компаний с активным онлайн-присутствием.

Социальная инженерия. Социальная инженерия — это манипуляции людьми для получения доступа к данным или системам компании. В настоящее время злоумышленники активно используют звонки, имитируя техподдержку или сотрудников банка, чтобы выманить конфиденциальную информацию. Например, участились случаи, когда атакующие звонят сотрудникам с просьбой назвать код подтверждения от мобильного банка.

В России информационная безопасность регулируется рядом законов, в которых установлено, как правильно работать с информацией: кто отвечает за ее сохранность, как ее собирать, обрабатывать, хранить и распространять.

Так, например, Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149 является главным законом об информации в России. В нем прописаны основные понятия в сфере информационной безопасности, требования к защите информации и ответственность за нарушения при работе с ней [7].

Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ регулирует работу с персональными данными [7].

Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ касается электронной подписи — цифрового аналога физической подписи, который помогает подтвердить подлинность информации и избежать ее искажения и подделки [9].

Одной из проблем российского законодательства является отсутствие полноты регулирования киберпреступлений. В настоящее время отсутствуют специальные структуры, осуществляющие полный контроль за незаконной деятельностью в сфере информационных технологий.

В связи с этим каждой организации любой формы собственности необходимо самостоятельно определять и реализовывать стратегию информационной безопасности.

Экономическая обоснованность. Любым компаниям, которые не уделяют внимания вопросам ИБ, грозит как минимум хищение ценной информации, а как максимум — ее недоступность.

Влияние геополитической напряженности так же имеет сильное влияние на количество кибератак, нацеленных как на государственные, так и на частные организации.

По прогнозам Cybersecurity Ventures, в 2024 году киберпреступность обойдется миру в 9,5 триллиона долларов США. В течение следующих двух лет ущерб от киберпреступлений в мире будет расти на 15% в год и к 2025 году достигнет 10,5 триллионов долларов США в год по сравнению с 3 триллионами долларов США в 2015 году.

Сегодня информация — это ключевой актив для любого бизнеса. Вместе с тем растет профессионализм мошенников, у хакеров появляются все новые инструменты для взлома, включая искусственный интеллект.

На фоне растущих угроз на первый план выходят эксперты по информационной безопасности, потребность в которых растет от года к году. Однако и здесь существует проблема, присущая малому предпринимательству в России.

В целом существуют направления деятельности, которые понятны владельцам компании и ее сотрудникам. К таким направлениям можно отнести, к примеру, направление сертификации и обеспечение продуктовой безопасности. В данной области сотрудник может показать результат своего труда — более безопасный продукт, сертификат соответствия и т. п.. Этот результат труда компания может обернуть в прибыль. Так, получив сертификат соответствия одного из регуляторов в нашей стране, можно открыть новые рынки для сбыта своей продукции, увеличивается штат заказчиков и прибыль.

Проблема направления информационной безопасности заключается в том, что никто, включая владельцев компании, не видит и не понимает результата их работы.

Коллеги считают, что специалисты отдела информационной безопасности необоснованно внедряют различные правила и системы, которые усложняют жизнь всех сотрудников компании, руководство зачастую смотрит на таких сотрудников без понимания результатов. Как оценить уровень безопасности? Что должно произойти, чтобы я почувствовал, за что я заплатил деньги? Подразделение информационной безопасности не приносит дохода, а расходы измеряются иногда сотнями тысяч и даже миллионов рублей. Однако при отсутствии таких расходов компания может потерять гораздо больше: ущерб и уничтожение данных, украденные деньги, потерю производительности, кражу интеллектуальной собственности, кражу личных и финансовых данных, растрату, мошенничество, нарушение нормального хода бизнеса после кибератаки, криминалистическую экспертизу, восстановление и удаление взломанных данных и систем, репутационный ущерб, судебные издержки и, возможно, немалые штрафы и претензии регулирующих и контролирующих органов.

Практическая значимость. На данный момент существует множество методов кибербезопасности для уменьшения количества кибератак и защиты данных от потери и компрометации данных.

Рассмотрим некоторые из практик кибербезопасности для современного бизнеса:

1. Реализация стратегии кибербезопасности. Одной из наиболее полезных практик кибербезопасности является реализация надежной стратегии кибербезопасности, необходимо на постоянной основе проводить аудиты кибербезопасности предприятия для оценки текущей ситуации.

2. Обеспечение резервного копирования данных и своевременность обновления для системы безопасности. Предприятия в современных условиях собирают огромные объемы данных о пользователях и заказчиках, что дополнительно требует от них стратегического подхода к резервному копированию своих данных, а также к использованию и управлению созданными копиями. Таким образом, сотрудники организации должны быть обучены и обязаны обновлять используемое программное обеспечение всякий раз, когда доступны обновленные версии, что помогает повысить информационную безопасность.

3. Сотрудничество с ИТ-подразделениями и специалистами. Предприятие получает преимущество от работы с ИТ-отделом, данная мера призвана предотвратить возникновение угроз и рисков от возможных кибератак. Превентивные меры различны для каждой конкретной организации и определяются целым рядом обстоятельств, тесное сотрудничество с штатными или сторонними ИТ-специалистами необходима для разработки стратегий информационной безопасности, таких как необходимость использования облачных технологий и какие типы мер безопасности было бы полезно принять.

4. Контроль над доступом к частной информации. Необходимо настроить управление доступом к информации, что включает в себя регулирование доступа к паролям безопасности, персональным данным, коммерческой информации и другим ресурсам. Необходимо разграничить уровни доступов к разным видам информации в компании. В результате лишь нескольким сотрудникам предоставляется доступ к финансовой информации компании и коммерческим секретам. Большинство сотрудников организации должны иметь доступ к личным данным и информации компании только по зарегистрированному запросу или на определенных условиях.

5. Использование образования и тренингов в области ИТ. Это еще одна важная и полезная передовая практика в области кибербезопасности. Следует проводить обучение по кибербезопасности и информационным технологиям, особенно когда сотрудники проходят адаптацию при трудоустройстве. Постоянное обучение, обновления программных продуктов и ИТ-поддержка должны быть неотъемлемой частью рабочих процессов, чтобы продолжать обеспечивать принятие и соблюдение мер кибербезопасности. Следует повышать осведомленность своих сотрудников о том, что они обязаны соблюдать правила кибербезопасности.

6. Обновление политики безопасности. Предприятия и организации должны регулярно обновлять свои правила безопасности, поскольку различные отделы и функции постоянно адаптируются к новым технологиям, инструментам и данным. Поэтому крайне важно иметь актуальную политику

безопасности, которая должна регулярно обновляться. Сотрудники должны быть обучены соблюдению каждого изменения политики безопасности.

7. Использование многофакторной аутентификации и надежных паролей. Обычные пользователи Интернета должны быть знакомы с требованиями к паролю, такими как использование прописных и строчных букв, цифр и символов, для разработки надежных паролей. Системы компаний и инструменты, как правило, имеют одинаковые потребности. Необходимо предоставлять пользователям сложные пароли для обеспечения максимальной безопасности. Другой тип защиты информации - многофакторная аутентификация, когда пользователям необходимо подтвердить свою личность на двух разных устройствах.

8. Мониторинг сторонних пользователей и приложений. Сторонние пользователи, имеющие доступ к приложениям и информационным системам организации, могут похитить данные, независимо от того, делают они это намеренно или нет. Любой из способов приводит к нарушениям кибербезопасности. Таким образом, отслеживая активность пользователей, заботясь об ограничении доступа к конфиденциальной информации и предоставляя одноразовые пароли, можно своевременно обнаруживать вредоносную активность, а также предотвращать возникновение взломов и несанкционированного доступа.

9. Игнорирование ссылок, всплывающих окон и ненужных сообщений. Одним щелчком мыши или нажатием клавиши клавиатуры пользователи могут позволить хакеру получить доступ к сетям компании. Поэтому важно быть очень осторожным с вложениями, ссылками и электронными письмами от неизвестных отправителей. Таким образом, сотрудники никогда не должны указывать какие-либо личные данные или информацию о компании в своих ответах на всплывающие окна, подозрительные электронные письма и сообщения. Нелишним будет внедрение технологии аутентификации электронной почты, которая блокирует подобные подозрительные электронные письма или сообщения.

10. Отслеживание действий привилегированных пользователей. Привилегированные пользователи являются одними из самых важных людей в бизнесе, но они также могут представлять наибольшую угрозу безопасности данных. Пользователи привилегированных учетных записей имеют специальный доступ, который может быть использован злоумышленниками и привести к повреждению, хищению и компрометации данных. В связи с этим необходимо ограничить количество привилегированных пользователей и убедиться, что привилегированные учетные записи деактивируются немедленно при совершении любых подозрительных действий. Чтобы фиксировать любые подозрительные действия внутри сети, необходимо включить решения для мониторинга активности пользователя.

11. С осторожностью использовать IP-адреса при входе в банковские онлайн-системы и при отправке отчетности в контролирующие органы. Если учет ведется по нескольким предприятиям, разграничение IP-адресов

предотвратит претензии контролирующих органов, и, возможно, судебные разбирательства с ними.

12. В связи с современной геополитической обстановкой и действующими на данный момент санкциями, большое количество производителей программного обеспечения покинули российский рынок. Российские компании вынуждены менять информационную инфраструктуру и переходить на отечественные или Open Source решения. При выборе таких решений для своей организации необходимо обратить внимание на то, как часто устраняются уязвимости в выбранном продукте, как часто выпускаются его обновления, есть ли у продукта поддержка, или же придется выполнять устранение обнаруженных недостатков своими силами в случае, если это Open Source решение, а так же совместим ли продукт с системным ПО, которое функционирует в организации.

Выводы. Информация была, есть и будет частью жизни общества, для предприятия информация – один из наиболее важных активов. Вопрос защиты информации всегда был актуален, будь то шифрование писем в прошлых столетиях или криптографические средства защиты сейчас – цель всегда будет преследоваться одна: защитить имеющиеся данные от хищения и компрометации. В современных условиях информационного общества этот вопрос стоит особенно остро, так как современные реалии развития информационных отношений подразумевают широкое использование и высокую ценность информации, а значит огромный поток передаваемой информации всегда будет подвергаться недобросовестной деятельности.

Учитывая статистику и новостные сообщения, не вызывает сомнений, что предприятиям необходимы адекватные меры безопасности для защиты своих данных, активов и операций от кибератак. Кибербезопасность бизнеса – задача первостепенной важности, но текущий ландшафт информационных угроз постоянно меняется, поэтому крайне необходимо отслеживать происходящие изменения в сфере цифровой безопасности, применять превентивные меры безопасности и своевременно реагировать на вновь возникающие угрозы.

Библиографический список

1. Лопатова Н. Кибербезопасность как фактор роста бизнеса // Наука и инновации. 2021. №3 (217)
2. Менисов А. Б. Киберщит. Искусственный интеллект и кибербезопасность. М., Алматы: Ай Пи Ар Медиа, 2024
3. Багдасарян, Г. Ф. Кибербезопасность и киберугрозы современного малого и среднего российского бизнеса // Вестник евразийской науки. 2023. Т. 15. № S2
4. Журнал о киберэкономическом рынке "Cybercrime Magazine" // Официальный сайт. URL: <https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/> (дата обращения: 18.11.2024)

5. Российская ежедневная деловая газета «Ведомости» // Официальный сайт.
URL: <https://www.vedomosti.ru/technology/news/2024/09/25/1064511-uscherb-kiberprestuplenii-previsil> (дата обращения: 18.11.2024)
6. Мазеин А. В. Правовое регулирование обеспечения кибербезопасности цифровых финансовых активов в России / А. В. Мазеин, С. С. Сметанина // Актуальные аспекты развития науки и общества в эпоху цифровой трансформации (шифр –МКАА): сборник материалов IX международной научно-практической конференции, Москва, 25 июля 2023 года. М.: Общество с ограниченной ответственностью "Издательство АЛЕФ". 2023. С. 46-55.
7. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 18.11.2024)
8. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149 URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 18.11.2024)
9. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ
URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 18.11.2024)