**Нгуен Као Бач - 15.27Д-БИ19/22б**

**Эссе**

**на тему <<Цифровая экономика перед вызовами кибератак и задачами управления информационной безопасностью в компаниях>>**

Цифровая экономика формируется и меняет привычные представления о том, как организованы предприятия, как компании взаимодействуют друг с другом и как потребители получают услуги, информацию и товары. Цифровая экономика ярко отражает переход от третьей промышленной революции к четвертой.

**Цифровая экономика — экономика, основанная на технологиях**

Цифровая экономика — это экономика, основанная на использовании цифровых технологий. Она применяет такие технологии, как Интернет, Всемирная паутина и вычислительная техника, для осуществления бизнес-операций, создавая экосистему, которая значительно превосходит традиционные понятия, такие как Интернет-экономика или Веб-экономика.

Стремительное развитие цифровой экономики стирает границы между цифровой и традиционной экономикой, объединяя людей, предприятия, устройства, данные и процессы в единую систему. Передовые технологии, такие как IoT, анализ больших данных, беспроводные сети и социальные сети, играют ключевую роль в модернизации платформ и создании новых бизнес-моделей.

Тем не менее, из-за высокой зависимости от технологий, особенно информационно-коммуникационных технологий (ИКТ), цифровая экономика сталкивается с серьёзными вызовами в области кибербезопасности и защиты данных.

**Цифровая экономика перед вызовами роста киберпреступности**

Рост цифровой экономики сопровождается увеличением угроз кибератак, которые становятся всё более доступными благодаря открытой продаже инструментов и методов взлома, а также уязвимостей в аппаратных и программных системах. Даже люди без специальной подготовки, включая несовершеннолетних, могут случайно нанести серьёзный ущерб организациям. Киберпреступность, одна из наиболее быстро развивающихся форм преступлений, представляет собой серьёзный вызов, с которым человечество столкнётся в ближайшие десятилетия.

Кибератаки эволюционировали от простых компьютерных вирусов 1980-х годов до сложных атак шестого поколения, таких как WannaCry и NotPetya. С ростом объёма распределённых данных эти атаки становятся всё сложнее для предотвращения и имеют более глубокие последствия.

Киберпреступники могут быть кем угодно: правительствами, организациями или частными лицами. Их цели варьируются от получения экономической выгоды до реализации политических или разрушительных намерений. Отсутствие географических и временных ограничений в цифровой экономике создаёт преимущество для злоумышленников, усиливая вызовы в области кибербезопасности. Хотя правительства вводят строгие меры контроля, это иногда вызывает негативную реакцию общества и влияет на социально-экономическую жизнь страны.

**Цифровая экономика и проблемы защиты данных и права пользователей на конфиденциальность**

В цифровой экономике все товары и услуги связаны с персональными данными пользователей. Владение физическими активами постепенно заменяется управлением цифровыми строками, кодами и символами. Сегодня банковский счёт и пароль к нему могут заменить сейф с наличными деньгами. Злоумышленникам больше не нужно взламывать сейфы — они могут украсть личные данные и финансовую информацию, такие как номера банковских счетов, кредитных карт или другие конфиденциальные данные, сидя за компьютером. Эти данные часто продаются или передаются другим киберпреступникам.

Защита персональных данных важна не только для безопасности пользователей, но и для функционирования всей экономики на макроуровне. Использование данных, будь то для продажи третьим лицам или для улучшения продуктов и услуг компаний, стало неотъемлемой частью современных бизнес-моделей.

Технологии, такие как искусственный интеллект (AI) и Интернет вещей (IoT), предлагают пользователям больше удобств, индивидуализации и выбора, но одновременно увеличивают риски, связанные с конфиденциальностью и кибербезопасностью. IoT соединяет различные устройства — от персональных компьютеров, бытовой техники, автомобилей до роботов и умных часов, создавая гигантский поток данных, включающий личную информацию и связи пользователей.

Поэтому компании, предоставляющие услуги на основе IoT, должны рассматривать безопасность как обязательный элемент качества. Современная экономика рассматривает пользовательские данные как ценный ресурс, сравнимый с "нефтяным месторождением". Основная задача заключается в том, чтобы безопасно и эффективно использовать этот ресурс, обеспечивая выгоду и соблюдение интересов всех заинтересованных сторон.

**Цифровая экономика и построение доверия**

Доверие и уверенность в цифровой экономике строятся на основе защиты личной информации, безопасности данных, ответственности за прозрачность работы и соблюдения стандартов управления цифровыми продуктами и услугами. Когда личные данные используются неправомерно, нарушается право на конфиденциальность, или распространяется недостоверная информация, это подрывает общественное доверие. Такой спад доверия замедляет развитие цифровой экономики и вносит нестабильность в общество, государство и рынки.

Чтобы сохранить доверие, организации и государства должны обеспечить три ключевых аспекта: прозрачность в использовании данных, справедливый обмен ценностями за предоставленную информацию и обязательство защищать данные клиентов. Прозрачность играет решающую роль в укреплении доверия, а обмен данными должен приносить обоюдную выгоду.

В условиях, когда личные данные становятся активом бизнеса, соблюдение обязательств по их защите становится жизненно важным. Нарушения в этой области подрывают доверие клиентов, что приводит к снижению репутации и рыночной стоимости бренда. Потерянное доверие восстановить крайне сложно. Поэтому компании должны сосредоточиться на построении доверия через предоставление качественных услуг и эффективное управление бизнесом.

**Задача управления рисками информационной безопасности в компаниях**

Можно утверждать, что с развитием цифровой экономики количество кибератак на предприятия также увеличивается. Полностью предотвратить такие атаки невозможно. Таким образом, главной задачей для компаний становится не только предотвращение и устранение инцидентов кибербезопасности, но и подготовка стратегий минимизации рисков после их возникновения. Управление рисками информационной безопасности стало одной из первоочередных задач для организаций и правительств в XXI веке.

**Компании должны формировать культуру управления рисками информационной безопасности (ИБ)**

Управление рисками информационной безопасности требует осознания на всех уровнях организации — от высшего руководства до рядовых сотрудников. Создание культуры осведомленности о кибербезопасности и вовлечение всех членов компании помогает увеличить шансы на успех всех планов по управлению рисками и обеспечивает долгосрочную стратегию управления.

Инвестиции в обучение и повышение осведомленности являются необходимыми для всех компаний, работающих в цифровой экономике. Даже если компания имеет отличных экспертов по безопасности, атаки могут быть совершены через обман других сотрудников с использованием методов социальной инженерии, таких как фишинговые письма или ложные запросы от имени руководства.

Любая ошибка — будь то охранника или бухгалтера — может поставить под угрозу безопасность сети компании. Поэтому сотрудники должны не только знать о возможных рисках, но и понимать, как их распознавать, что делать и к кому обращаться при обнаружении подозрительных действий.

Помимо защиты от внешних угроз, регулярная "очистка" внутренней сети также играет важную роль. Это подразумевает ежедневное соблюдение процедур проверки, мониторинга и корректировки, чтобы система компании оставалась в безопасности. Такие процессы требуют инвестиций во время и средства для создания специализированных отделов.

Культура управления рисками также выражается в готовности руководства учитывать разные мнения для поиска оптимальных решений. Привлечение сторонних экспертов для объективной оценки и поиска уязвимостей в стратегии управления рисками является разумным и полезным шагом для повышения эффективности.

**Компании должны проводить оценку рисков информационной безопасности (ИБ)**

Процесс оценки рисков информационной безопасности в компании аналогичен процессу оценки любых других бизнес-рисков, с которыми может столкнуться организация. Основные элементы оценки рисков включают определение вероятности возникновения риска и анализ последствий события, если оно произойдет. На основе этого разрабатываются и реализуются меры по снижению вероятности или серьезности каждого потенциального риска.

Оценка рисков в области информационной безопасности заключается в понимании, управлении, контроле и минимизации этих рисков в масштабах всей организации. Ключевым этапом является проверка данных. Согласно отчету IBM "Cost of a Data Breach 2020", средняя глобальная стоимость одного утечки данных составляет 3,9 миллиона долларов США. Утечка данных считается одним из самых затратных видов кибератак, поскольку данные компании являются одним из ее самых ценных активов. Поэтому проверка данных является важнейшим этапом в процессе оценки рисков информационной безопасности.

**План реагирования на инциденты: ключевые шаги и важность киберстрахования**

План реагирования на инциденты — это набор инструкций, описывающих конкретные шаги, которые необходимо предпринять в случае кибератаки. Эффективный план позволяет оперативно реагировать и минимизировать время и потенциальные последствия любых атак.

Такой план обычно включает 11 этапов: изоляция угрозы для предотвращения её распространения, проверка данных для оценки потерь и выявления возможных рисков, удаление заражённых файлов и, при необходимости, замена аппаратного или программного обеспечения. Необходимо вести подробный журнал событий и реагирования, оперативно информировать клиентов и партнёров о затронутых данных, консультироваться с юридическим отделом относительно возможных рисков и нормативных последствий, а также уведомлять полицию, поскольку атака может затронуть не только одну компанию. Дополнительно следует восстановить систему в её первоначальное состояние, мониторить ситуацию, извлекать уроки и продолжать оценку эффективности выполненного плана.

Киберстрахование становится необходимостью для компаний, работающих в цифровой экономике.

**Роль киберстрахования в управлении рисками**

В современном обществе растущая сложность цифровой среды требует внимания к страхованию. В области кибербезопасности многие компании предлагают услуги страхования, чтобы помочь бизнесу справляться с рисками.

Несмотря на наличие стратегий управления рисками, не все угрозы можно предотвратить или смягчить. Именно поэтому компании должны максимально передавать риски третьим сторонам через приобретение бизнес-страховок.

Среди самых важных мер защиты от рисков в области информационной безопасности выделяются два вида страхования: киберстрахование и страхование от ошибок и упущений в технологиях.

Полисы киберстрахования позволяют компаниям переложить часть потенциальных затрат, связанных с восстановлением после кибератак или других инцидентов, негативно влияющих на безопасность. Страхование от ошибок и упущений в основном приобретается разработчиками программного обеспечения.

Эти два вида страхования являются важными элементами общей программы и стратегии управления рисками информационной безопасности компании. Стоимость полиса киберстрахования зависит от множества факторов, включая размер организации, отрасль и степень её зависимости от технологий.

**Заключение**

Киберриски — это неотъемлемая часть современного бизнеса, неизбежная плата за работу в цифровую эпоху. Методы защиты должны быть эффективнее инструментов, которыми пользуются злоумышленники.

В цифровой экономике существует не только рынок товаров и услуг, несущий пользу человечеству, но и параллельный теневой рынок киберпреступности. На этом рынке доступны инструменты для атак, включая эксплойты уязвимостей, кастомизированное вредоносное ПО и аренду ботнетов. Это позволяет даже подросткам с минимальными знаниями проводить атаки с использованием программ-вымогателей. Профессиональные киберпреступники могут зарабатывать до 2 миллионов долларов в год, средний уровень дохода составляет 900 тысяч долларов, а начинающие хакеры получают около 42 тысяч долларов.

**Необходимость немедленных действий**

Настало время компаниям действовать. Доверие необходимо выстраивать. Цифровая экономика, как будущее человечества, немыслима без стратегических и глобальных мер по обеспечению информационной безопасности.

Во Вьетнаме на данный момент отсутствуют нормативные акты или рекомендации государственных органов, направленные на разработку и внедрение стратегий и мер управления рисками информационной безопасности для бизнеса.

**Интеграция управления рисками в процессы бизнеса**

Управление рисками информационной безопасности является неотъемлемой частью общей системы управления рисками как для деятельности компаний, так и для экономической и социальной сферы в условиях современной цифровой экономики. Министерство информации и коммуникаций Вьетнама, как государственный регулятор и координатор цифровой трансформации, получивший поручение от премьер-министра на разработку Национальной стратегии цифровой экономики и цифрового общества, должно предоставить компаниям рекомендации по управлению рисками информационной безопасности.

**Рекомендации для создания комплексной системы**

Эти рекомендации должны представлять собой прозрачную, гибкую и системную процедуру, обеспечивающую эффективное управление киберрисками в рамках общей стратегии управления рисками. Такой подход будет способствовать достижению экономических и социальных целей страны, укрепляя доверие к цифровой экономике.