Аннотация – В рамках анализа ситуации с кибербезопасностью в Азиатско-Тихоокеанском регионе (APAC) на 2023 год в этом документе рассматриваются различные аспекты киберугроз, которые оказали значительное влияние на регион. На регион приходится 31% глобальных кибератак, и он превратился в центр киберпреступной деятельности, причём более половины его организаций становятся жертвами этих угроз. Этот анализ направлен на то, чтобы обеспечить качественный синтез преобладающих угроз кибербезопасности, опираясь на информацию из различных исследований и отчётов, чтобы предложить целостное представление о вызовах и уязвимостях, с которыми сталкивается регион.

Выводы, полученные в результате этого анализа, имеют важное значение для специалистов в области кибербезопасности, ИТ-специалистов-практиков и заинтересованных сторон в различных секторах, предоставляя им более глубокое понимание проблем и вооружая их знаниями для совершенствования их стратегий защиты от меняющегося ландшафта киберугроз.

I. Введение

В 2023 году Азиатско-Тихоокеанский регион (APAC) столкнулся с множеством угроз кибербезопасности. На этот регион пришлось 31% глобальных кибератак, при этом более половины всех организаций региона сообщили, что они подвергались кибератакам.

Конкретные угрозы, нацеленные на регион в 2023 году, включали кампанию социальной инженерии группы Kimsuky по краже учётных данных, использование группой UNC4841 уязвимости нулевого дня и использование вредоносного ПО RDStealer, нацеленного на протокол удаленного рабочего стола.

В отчете Thales Data Threat Report также подчёркивается, что 60% респондентов из региона назвали расшифровку сети угрозой безопасности квантовых вычислений, вызывающей наибольшую озабоченность. Кроме того, 50% организаций региона имели официальный план реагирования на программы-вымогатели по сравнению с 47% в 2022 году.

Рост числа кибератак угрожает жизненно важным секторам экономики Азии, которые становятся более уязвимыми по мере продолжения цифровой трансформации. Несмотря на увеличение количества специалистов по кибербезопасности в регионе, по-прежнему существует нехватка подготовленных сотрудников, которая оценивается в 2,16 миллиона человек.

II. Топ угроз:

- Фишинг
- Инфостилеры
- Методы обхода MFA
- Программы-вымогатели
- Supply-chain атаки
- Атаки, мотивированные хактивизмом
- Риски генеративного ИИ.

Фишинг остаётся одной из наиболее распространённых киберугроз в регионе, при этом число инцидентов значительно возросло. Киберпреступники использовали различные методы, такие как SMS (смишинг), вишинг и выдачу себя за другое лицо в социальных сетях, чтобы обманом заставить людей разгласить конфиденциальную информацию. Использование генеративных технологий искусственного интеллекта, таких как ChatGPT, ещё больше усилило эти фишинговые кампании, позволяя злоумышленникам создавать более убедительный и целевой фишинговый контент.

InfoStealers, вредоносное ПО, предназначенное для сбора и кражи конфиденциальных данных из систем жертв, продемонстрировали повышенную активность. Эти угрозы были нацелены на широкий спектр данных, включая личную идентификационную информацию, финансовые данные и учётные данные для входа в систему, создавая значительные риски как для отдельных лиц, так и для организаций.

Несмотря на широкое распространение многофакторной аутентификации (MFA) в качестве меры безопасности, киберпреступники разработали и использовали различные методы обхода защиты MFA. Эти методы использовали уязвимости в реализации систем MFA, с целью получения конфиденциальной информации.

Атаки программ-вымогателей резко возросли, при этом увеличилось количество инцидентов, направленных против предприятий и критической инфраструктуры. В рамках атак происходило не только шифрование данных, но и их кража, что удваивало давление вымогательства на жертв.

В регионе наблюдался рост числа chain-атак, когда киберпреступники проникали в системы программного обеспечения на этапе создания или обновления. Эти атаки позволили злоумышленникам распространять вредоносное

ПО среди пользователей скомпрометированного программного обеспечения, подчёркивая уязвимости в процессах разработки и распространения программного обеспечения.

Хактивизм набрал силу в регионе и были нацелен на правительственные учреждения, корпорации и другие организации, движимые различными политическими, социальными и экологическими мотивами. Последствия этих атак варьировались от утечек данных до разрушительных атак типа «отказ в обслуживании».

Потенциальное злоупотребление генеративными технологиями искусственного интеллекта стало новой угрозой кибербезопасности. Эти технологии могут быть использованы для автоматизации и усиления кибератак, включая фишинг, создание контента для вредоносных целей и создание дипфейков. Быстрое развитие технологий искусственного интеллекта потребовало переоценки стратегий кибербезопасности для борьбы с этими возникающими угрозами.

Угрозы кибербезопасности, с которыми столкнулся регион в 2023 году, имели серьёзные экономические и стратегические последствия. Прямые финансовые потери от кибератак, сбоев в работе, репутационного ущерба и увеличения затрат на кибербезопасность создали проблемы для экономической стабильности и роста региона. Более того, стратегические последствия спонсируемой государством кибердеятельности и атак на критически важную инфраструктуру подчёркивают важность национальной и региональной устойчивости кибербезопасности.

III. Последствия кибератак в Азиатско-Тихоокеанском регионе

Кибератаки в регионе имеют серьёзные последствия, затрагивающие как организации, так и отдельных лиц. Эти последствия подчёркивают необходимость более активных усилий по обеспечению кибербезопасности в регионе, включая увеличение инвестиций, улучшение возможностей обнаружения и реагирования, а также большую прозрачность в отношении кибератак.

- **Компрометация конфиденциальной информации.** Примерно 49% успешных атак на организации привели к компрометации конфиденциальной информации. Сюда могут входить персональные данные клиентов или сотрудников, финансовые данные или конфиденциальная деловая информация.
- **Нарушение основных операций.** В 27% случаев жертвы пострадали от сбоев в основных операциях, включая приостановку бизнес-процессов и услуг. Это может привести к значительным финансовым потерям и ущербу репутации организации.
- **Экономический потери:** если не будут приняты меры по повышению стандартов кибербезопасности, азиатские страны будут продолжать сталкиваться с экономическими потерями от кибератак каждый год.
- **Задержка обнаружения и реагирования.** Организациям в регионе требуется в 1,7 раза больше времени, чем в среднем по миру, чтобы обнаружить нарушение. Эта задержка может позволить злоумышленникам нанести больший ущерб или украсть больше информации.
- **Недостаточная осведомленность о кибербезопасности и инвестиции:** 70% организаций в регионе не имеют четкого понимания своей кибер-позиции, а инвестиции в кибербезопасность в регионе на 47% ниже, чем в Северной Америке. Отсутствие осведомленности и инвестиций может сделать организации более уязвимыми для атак.
- **Отсутствие прозрачности.** Многие кибератаки не разглашаются из-за репутационных рисков. Отсутствие прозрачности может помешать региону осознать весь масштаб угрозы и эффективно отреагировать.
- **Ответственность правительства:** правительство региона также несут ответственность за слабую кибербезопасность в регионе, при этом в некоторых странах действуют более комплексные законы о защите данных и кибербезопасности, чем в других.

IV. Экономические последствия

- **Финансовые потери:** около 63% организаций в регионе сообщили о финансовых последствиях из-за киберинцидентов. Точные денежные потери могут широко варьироваться в зависимости от характера и масштаба атаки, но они могут включать в себя прямые затраты, такие как выкуп, ремонт и восстановление системы, а также косвенные затраты, такие как потеря дохода из-за простоя.
- **Нарушение основных операций.** В 27% случаев жертвы пострадали от сбоев в основных операциях, включая приостановку бизнес-процессов и услуг. Это может привести к значительным эксплуатационным расходам и снижению производительности.
- **Репутационный ущерб:** публичное признание нарушения обычно влечет за собой значительный репутационный ущерб в дополнение к повреждению систем. Это может привести к потере доверия клиентов и потенциальному снижению бизнеса, что может иметь долгосрочные экономические последствия.
- **Экономический саботаж.** атаки направлены на экономический саботаж, который может иметь широкомасштабные последствия для экономики страны или региона.
- **Нарушения в цепочках поставок.** могут вызвать сбои в цепочках поставок, что может привести к росту цен и экономической нестабильности.
- **Потеря рабочих мест.** крупная кибератака может привести к значительной потере рабочих мест. Например, уровень безработицы может вырасти до

5,7% в первом квартале после крупной атаки, что эквивалентно потере 3,1 миллиона рабочих мест.

- **Инвестиционные потери:** возможность потерять в общей сложности 2,884 миллиарда долларов США (в реальном выражении) инвестиций за 5 лет.
- **Увеличение затрат на кибербезопасность:** по мере роста киберугроз организациям и правительствам необходимо больше инвестировать в меры кибербезопасности, что может стать значительным экономическим бременем.
- **Репутационный ущерб:** репутационный ущерб от кибератаки может иметь долгосрочные последствия для ценности бренда компании и доверия клиентов, что потенциально может привести к снижению бизнеса и доходов.
- **Снижение кредитного рейтинга:** атака может привести к снижению кредитного рейтинга компании, что может увеличить стоимость заимствований и повлиять на её способность привлекать капитал.

В 2023 году наиболее пострадавшими от кибератак отраслями в регионе были:

- **Производство.** в отрасли зарегистрировано 48% случаев кибератак.
- **ИТ-компании:** входят в тройку наиболее целевых отраслей благодаря ценным данным, с которыми они работают, и быстрой цифровой трансформации в регионе.
- **Финансы и страхование.** сектор также подвергся серьёзным кибератакам.
- **Розничная торговля:** за последние 24 месяца произошло наибольшее количество успешных кибератак, в основном из-за нехватки бюджета на кибербезопасность.
- **Правительственные учреждения:** подвергались атакам, поскольку содержат ценную информацию, такую как личные данные граждан и информацию национального значения.
- **Промышленные компании:** подверглись нападению из-за потенциального экономического кризиса и кражи интеллектуальной собственности.
- **Фармацевтика и сельское хозяйство:** эти отрасли жизненно важны для экономики и национальной безопасности, что делает их привлекательными целями для киберпреступников.
- **Здравоохранение:** организации здравоохранения хранят конфиденциальную информацию и часто имеют ограниченные ИТ-ресурсы, что делает их уязвимыми для кибератак.
- **Образование/исследования:** этот сектор подвергся наибольшему количеству атак: в среднем 2160 атак на организацию в неделю.

A. Производство

Непосредственные финансовые и операционные последствия

- **Прямые финансовые потери:** крупные производственные компании в регионе могут потерять в среднем 10,7 миллионов долларов США из-за кибератаки. Эти потери включают в себя как прямые затраты, такие как потеря производительности, штрафы и затраты на исправление ситуации, так и косвенные затраты, (отток клиентов из-за репутационного ущерба).
- **Операционные сбои.** атаки могут нарушить производственные операции, что приведет к простоям и снижению производительности. Сложность управления большим портфелем ИБ-решений может привести к увеличению времени восстановления после кибератак, что ещё больше усугубляет сбои в работе.
- **Нарушения в цепочке поставок.** организации не только теряют время и ресурсы на борьбу с последствиями атаки, но также может быть нарушена вся цепочка поставок, что затронет как организацию, так и ее партнеров.

Долгосрочные экономические и стратегические последствия

- **Задержка цифровой трансформации.** три из пяти производственных организаций в регионе задержали ход цифровой трансформации из-за проблем с кибербезопасностью. Эта задержка ограничивает возможности производственных организаций защищаться от кибератак и использовать новые технологии, такие как искусственный интеллект, облака и Интернет вещей, для повышения производительности и предоставления новых линий обслуживания.
- **Компрометация конфиденциальной информации.** Производственные организации подвергаются нападениям из-за своих ценных данных, включая интеллектуальную собственность и конфиденциальную оперативную информацию. Компрометация таких данных может иметь серьёзные последствия для конкурентных преимуществ и позиционирования на рынке.
- **Повышенная кибербезопасность затраты.** Чтобы защититься от растущих угроз, производственным организациям необходимо больше инвестировать в меры кибербезопасности, что может стать значительным экономическим бременем. Это включает в себя инвестиции в возможности искусственного интеллекта и машинного обучения для автономного выявления киберугроз и улучшения их обнаружения и реагирования.

Отраслевые уязвимости

- **Цель по экономическому разрушению и краже интеллектуальной собственности.** Производственный сектор особенно уязвим из-за

его решающей роли в экономике и потенциального экономического кризиса и кражи интеллектуальной собственности.

Стратегии реагирования и смягчения последствий

- **Укрепление кибербезопасности с помощью ИИ.** ИИ играет решающую роль, позволяя организациям защищаться от все более сложных киберугроз. Решения кибербезопасности, дополненные возможностями ИИ и машинного обучения, могут помочь быстро выявлять угрозы за счёт обнаружения поведенческих аномалий и введения правил для блокировки или карантина устройств, ведущих себя неожиданно.

B. ИТ-компании

Непосредственные финансовые и операционные последствия

- **Прямые финансовые потери.** В ИТ-секторе региона наблюдается рост количества атак на веб-приложения и API на 36%, при этом произошло более 3,7 миллиардов атак. Эти атаки могут привести к существенным финансовым потерям из-за ремонта системы, затрат на восстановление и потенциальных штрафов за несоблюдение нормативных требований.
- **Сбои в работе.** атаки могут привести к значительным сбоям в работе ИТ, что приведет к простоям и снижению производительности. Сложность управления большим портфелем ИБ-решений может привести к увеличению времени восстановления после кибератак.

Долгосрочные экономические и стратегические последствия

- **Репутационный ущерб.** Публичное раскрытие информации о кибератаке может нанести ущерб репутации ИТ-компании, что приведет к потере доверия среди потребителей, партнеров и инвесторов. Это может иметь долгосрочные последствия для доли рынка и прибыльности.
- **Проблемы с нормативным регулированием и соблюдением требований.** Кибератаки могут привести к несоблюдению нормативных требований, что приведет к штрафам и судебным разбирательствам. Это особенно важно для ИТ-компаний, где соблюдение законов о защите данных и конфиденциальности клиентов имеет первостепенное значение.

Отраслевые уязвимости

- **Цель по краже данных и финансовой выгоде.** ИТ-сектор особенно уязвим из-за его роли в эпоху цифровой трансформации и ценных данных, с которыми он работает. Киберпреступники могут атаковать ИТ-компании, чтобы нарушить работу, украсть конфиденциальные данные или совершить финансовое мошенничество.

Стратегии реагирования и смягчения последствий

- **Увеличение затрат на кибербезопасность.** ИТ-компаниям необходимо инвестировать значительные средства в защитные меры. Это включает в себя усиление киберзащиты, проведение регулярных проверок безопасности и обучение персонала, что может стать существенным экономическим бременем.

C. Финансы и страхование

Непосредственные финансовые и операционные последствия

- **Прямые финансовые потери.** количество атак на веб-приложения и API увеличилось на 36%, что в общей сложности составило более 3,7 миллиардов атак. Эти атаки могут привести к прямым финансовым потерям из-за «ремонта» системы, затрат на восстановление и штрафов за несоблюдение нормативных требований.
- **Сбои в работе.** атаки могут привести к значительным сбоям в работе, простоям и снижению производительности. Сложность управления большим портфелем решений по кибербезопасности может привести к увеличению времени восстановления после кибератак.

Долгосрочные экономические и стратегические последствия

- **Репутационный ущерб.** Публичное раскрытие информации о кибератаке может нанести ущерб репутации финансового учреждения, что приведет к потере доверия среди потребителей, партнеров и инвесторов. Это может иметь долгосрочные последствия для доли рынка и прибыльности.
- **Проблемы с нормативным регулированием и соблюдением требований.** атаки могут привести к несоблюдению нормативных требований, штрафам и судебным разбирательствам. Это особенно важно для финансовых учреждений, где соблюдение законов о защите данных и конфиденциальности клиентов имеет первостепенное значение.

Отраслевые уязвимости

- **Цель по экономическим потрясениям и краже данных.** Финансовый и страховой сектор особенно уязвим из-за роли в экономике и потенциального экономического сбоя и кражи конфиденциальных данных. Атаки этот сектор, могут сорвать операции, украсть конфиденциальные данные или совершить финансовое мошенничество.

Стратегии реагирования и смягчения последствий

- **Увеличение затрат на кибербезопасность.** учреждениям необходимо инвестировать значительные средства в меры кибербезопасности. Это включает в себя усиление киберзащиты, проведение регулярных проверок безопасности и

обучение персонала, что может стать существенным экономическим бременем.

- **Регуляторные и репутационные риски:** контроль со стороны регулирующих органов и репутационные риски усилились по всему региону, при этом громкие утечки данных влияют на финансовые показатели, вызывают негативную проверку со стороны регулирующих органов, подрывают акционерную стоимость и подвергают риску корпоративных должностных лиц.

D. Розничная торговля

Непосредственные финансовые и операционные последствия

- **Прямые финансовые потери.** За последние 24 месяца в сфере розничной торговли в регионе произошло наибольшее количество успешных кибератак, в первую очередь из-за недостаточности бюджетов на кибербезопасность. Это привело к прямым финансовым потерям, включая затраты на «ремонт» и восстановление системы, а также потенциальным штрафам за несоблюдение нормативных требований.
- **Операционные сбои.** Кибератаки могут привести к серьёзным сбоям в работе розничной торговли, простоям и снижению производительности. Сложность управления большим портфелем ИБ-решений может привести к увеличению времени восстановления после кибератак.

Долгосрочные экономические и стратегические последствия

- **Репутационный ущерб.** Публичное раскрытие информации о кибератаке может нанести ущерб репутации розничной организации, что приведет к потере доверия среди потребителей, партнеров и инвесторов. Это может иметь долгосрочные последствия для доли рынка и прибыльности.
- **Проблемы с нормативным регулированием и соблюдением требований.** атаки могут привести к несоблюдению нормативных требований, что приведет к штрафам и судебным разбирательствам. Это особенно важно для организаций розничной торговли, где соблюдение законов о защите данных и конфиденциальности клиентов имеет первостепенное значение.

Отраслевые уязвимости

- **Цель по экономическим потрясениям и краже данных.** Сектор розничной торговли особенно уязвим из-за его критической роли в экономике и возможности экономического разрушения и кражи конфиденциальных данных. Атаки на розничные компании, могут нарушить их работу, украсть конфиденциальные данные или совершить финансовое мошенничество.

Стратегии реагирования и смягчения последствий

- **Увеличение затрат на кибербезопасность.** организациям необходимо инвестировать значительные средства в меры кибербезопасности. Это включает в себя усиление киберзащиты, проведение регулярных проверок безопасности и обучение персонала.

Дополнительные соображения

- **Атаки программ-вымогателей.** Сектор розничной торговли уязвим для атак программ-вымогателей, поскольку он обрабатывает большой объем транзакций по кредитным картам. Использование программ-вымогатели для шифрования важных данных приводит к требованию выкупа, что ещё больше усугубляет финансовые потери.
- **Вредоносные боты.** В коммерческом секторе также наблюдалось значительное количество вредоносных ботов, чему способствовало количество и частота праздничных торговых мероприятий, а также рост количества онлайн-бронирований путешествий. Однако в первом квартале 2023 года активность вредоносных ботов существенно снизилась.

E. Государственные органы

Непосредственные последствия для эксплуатации и безопасности

- **Компрометация конфиденциальной информации.** Госсистемы хранят огромное количество ценной информации, включая личные данные граждан, статистику и информацию национального значения. Злоумышленникам удалось похитить данные в 44% успешных атак на правительственные организации, что создало значительный риск для национальной безопасности и конфиденциальности личности.
- **Нарушение работы государственных служб.** атаки серьёзно нарушают работу правительства, что приведет к приостановке работы важнейших государственных служб, что имеет последствия для жизни граждан и экономики.

Финансовые затраты

- **Прямые и косвенные финансовые потери.** Финансовые последствия и включают в себя прямые затраты, такие как восстановление системы, и косвенные затраты, такие как потеря производительности и репутационный ущерб, что отвлекает ресурсы от основных госуслуг.

Репутационный ущерб

- **Потеря общественного доверия.** атаки подрывают доверие общества к государственным учреждениям. Восприятие неадекватных мер кибербезопасности может привести к снижению уверенности в способности правительства защитить конфиденциальную информацию и обеспечить общественную безопасность.

Проблемы регулирования и соблюдения требований

- **Несоблюдение правил:** атаки приводят к несоблюдению различных правил, касающихся защиты данных и конфиденциальности, что приведет к штрафам и судебным разбирательствам. Это особенно важно для государственных учреждений, которые придерживаются высоких стандартов защиты данных.

Угрозы национальной безопасности

- **Шпионаж и саботаж.** Правительственные учреждения являются основными объектами спонсируемого государством кибершпионажа и диверсий. Атаки приводят к краже конфиденциальной информации о нацональной безопасности или нарушению работы критически важной инфраструктуры, создавая серьёзную угрозу безопасности на уровне страны.

Долгосрочные стратегические последствия

- **Международные отношения и геополитическая напряжённость.** Атаки на правительственные учреждения могут иметь долгосрочные последствия для международных отношений, особенно если их приписывают субъектам иностранных государств. Подобные инциденты могут привести к эскалации геополитической напряженности и привести к ответным действиям.

- **Увеличение затрат на кибербезопасность.** правительственным учреждениям необходимо вкладывать значительные средства в меры кибербезопасности. Это включает в себя усиление киберзащиты, проведение регулярных проверок безопасности и обучение персонала, что может стать существенным экономическим бременем.

Влияние на цифровую трансформацию

- **Препятствие для инициатив цифрового правительства.** ИБ-инциденты замедляют прогресс цифрового правительства, направленных на улучшение государственных услуг с помощью технологий, что, в свою очередь, может привести к сложности внедрения новых цифровых решений.

F. Промышленные компании

Непосредственные финансовые и операционные последствия

- **Прямые финансовые потери:** крупные компании могут потерять в среднем 10,7 миллионов долларов США из-за кибератаки. Эти потери включают в себя прямые затраты: потеря производительности, штрафы, затраты на исправление ситуации, и косвенные затраты, такие как отток клиентов из-за репутационного ущерба.

- **Сбои в работе.** Атаки приводят к значительным сбоям в производственных операциях, простоям и снижению производительности. Сложность управления большим портфелем решений по кибербезопасности может привести к увеличению времени восстановления после кибератак.

- **Нарушения в цепочке поставок.** Вся цепочка поставок может быть нарушена в результате кибератак на производственные организации, затрагивающих не только целевую компанию, но и ее партнеров.

Долгосрочные экономические и стратегические последствия

- **Задержка цифровой трансформации:** почти три из пяти производственных организаций в регионе задержали ход цифровой трансформации. Эта задержка может ограничить их возможности по защите от кибератак и использованию новых технологий для повышения производительности и предоставления новых линий обслуживания.

- **Компрометация конфиденциальной информации.** Производственные организации часто подвергаются нападениям из-за своих ценных данных, включая интеллектуальную собственность и конфиденциальную оперативную информацию. Компрометация таких данных может иметь серьёзные последствия для конкурентных преимуществ и позиционирования на рынке.

Отраслевые уязвимости

- **Цель по экономическому разрушению и краже интеллектуальной собственности.** Производственный сектор особенно уязвим из-за его решающей роли в экономике и потенциального экономического кризиса и кражи интеллектуальной собственности. Киберпреступники и представители национальных государств могут атаковать этот сектор, чтобы сорвать операции, украсть конфиденциальные данные или провести промышленный шпионаж.

Стратегии реагирования и смягчения последствий

- **Укрепление кибербезопасности с помощью ИИ.** ИИ играет решающую роль, позволяя производственным организациям защищаться от все более сложных киберугроз. Решения кибербезопасности, дополненные возможностями искусственного интеллекта и машинного обучения, могут помочь быстро выявлять угрозы за счет обнаружения поведенческих аномалий и введения правил для блокировки или карантина устройств, ведущих себя неожиданно.

G. Фармацевтика и сельское хозяйство

Фармацевтический сектор

- **Кража интеллектуальной собственности.** Фармацевтический сектор является основной мишенью кибератак, направленных на кражу интеллектуальной собственности особенно в отношении формул лекарств и данных клинических испытаний. Такое воровство может

подорвать конкурентные преимущества и привести к значительным финансовым потерям.

- **Операционные сбои.** Кибератаки могут нарушить производственные процессы и цепочки поставок, что приведет к задержкам в производстве и распространении лекарств. Это может оказать прямое влияние на общественное здравоохранение, особенно если пострадает производство важнейших лекарств.
- **Финансовые потери.** Финансовые последствия кибератак на фармацевтические компании могут быть ошеломляющими: затраты, связанные с нарушениями, в среднем превышают 5 миллионов долларов США. Эти затраты включают в себя прямые расходы, такие как выплаты выкупа и восстановление системы, а также косвенные затраты, такие как потерянный доход и судебные издержки.
- **Репутационный ущерб.** Публичное раскрытие информации о кибератаке может нанести ущерб репутации фармацевтической компании, что приведет к потере доверия среди потребителей, партнеров и инвесторов. Это может иметь долгосрочные последствия для доли рынка и прибыльности.
- **Проблемы с нормативным регулированием и соблюдением требований.** Атаки приводят к несоблюдению нормативных требований, к штрафам и судебным разбирательствам. Это особенно важно в фармацевтической отрасли, где соблюдение законов о защите данных и конфиденциальности пациентов имеет первостепенное значение.

Сельскохозяйственный сектор

- **Нарушение операций.** Кибератаки могут нарушить сельскохозяйственную деятельность, затрагивая все: от мониторинга посевов до управления животноводством. Это может привести к снижению производительности и финансовым потерям для фермеров и агробизнеса.
- **Компрометация конфиденциальных данных.** Сельскохозяйственный сектор собирает и хранит огромное количество данных, от финансовых отчетов до информации об урожайности. Кибератаки могут поставить под угрозу эти данные, что приведет к нарушению конфиденциальности и финансовой краже.
- **Уязвимости цепочки поставок:** Сельскохозяйственный сектор глубоко интегрирован в глобальные цепочки поставок. Кибератаки могут разрушить эти цепочки, что приведет к нехватке продовольствия, росту цен и экономической нестабильности.
- **Финансовые последствия.** Затраты, связанные с восстановлением после кибератаки, включая выплаты выкупа, восстановление системы и усиление мер кибербезопасности, могут быть значительными для сельскохозяйственного бизнеса.
- **Репутационный ущерб.** Как и в фармацевтическом секторе, сельскохозяйственный бизнес может понести репутационный ущерб в результате кибератаки, что повлияет на доверие потребителей и деловые отношения.
- **Проблемы регулирования и соответствия:** сельскохозяйственные предприятия могут столкнуться с проблемами регулирования после кибератаки, особенно если атака приводит к несоблюдению правил безопасности пищевых продуктов и защиты данных.

H. Здравоохранение

Последствия кибератак на сектор здравоохранения в регионе глубоки и многогранны, они затрагивают не только непосредственные оперативные возможности медицинских учреждений, но также имеют долгосрочные последствия для доверия пациентов, финансовой стабильности и здравоохранения в целом. экосистема. Вот некоторые из ключевых эффектов:

Моментальный сбой в работе

Кибератаки могут серьёзно нарушить работу здравоохранения, мешая больницам оказывать своевременную помощь. Эти сбои могут быть особенно критичными во время чрезвычайных ситуаций в области здравоохранения, таких как пандемия COVID-19, когда спрос на медицинские услуги резко возрастает. Восстановление ИТ-систем и получение украденных данных часто требуют уплаты значительного выкупа, что ещё больше истощает ресурсы здравоохранения.

Компрометация конфиденциальных данных пациентов

Организации здравоохранения хранят огромные объемы конфиденциальных данных о пациентах, что делает их главной мишенью для киберпреступников. Компрометация таких данных может иметь серьёзные последствия для конфиденциальности пациентов и привести к краже личных данных и мошенничеству. Потеря конфиденциальных медицинских данных может привести к непоправимому репутационному ущербу, потере доверия и оттоку пациентов из медицинских организаций.

Финансовые потери

Экономические последствия кибератак на организации здравоохранения в регионе могут быть ошеломляющими. Инцидент кибератаки может стоить крупной организации здравоохранения примерно 23,3 миллиона долларов США. Сюда входят как прямые затраты, такие как потеря производительности, штрафы и затраты на исправление ситуации, так и косвенные затраты, такие как отток клиентов из-за репутационного ущерба.

Выкупные выплаты

Значительная часть медицинских организаций в регионе, ставших жертвами атак программ-вымогателей, в итоге выплачивают выкуп. Это не только обременяет

организации финансово, но и побуждает киберпреступников продолжать свою вредоносную деятельность.

Влияние на оказание медицинской помощи

Кибератаки могут оказать умеренное или серьёзное влияние на оказание медицинской помощи, ставя под угрозу здоровье и безопасность пациентов. В некоторых случаях лечение неотложной помощи, необходимое пациентам, может быть отложено, а неэкстренные случаи могут быть принудительно отменены, поскольку врачи и медицинский персонал не имеют доступа к жизненно важной информации о пациентах.

Проблемы регулирования и соблюдения требований

Сектор здравоохранения строго регулируется, и кибератаки могут привести к несоблюдению различных правил конфиденциальности и безопасности медицинской информации. Это может привести к огромным штрафам и судебным разбирательствам, что ещё больше усугубит финансовую нагрузку на организации здравоохранения.

Увеличение затрат на кибербезопасность

Чтобы защититься от растущих угроз, организациям здравоохранения необходимо инвестировать в меры кибербезопасности, что может стать значительным экономическим бременем. Это включает в себя инвестиции в людей, процессы и технологии, такие как обучение кибербезопасности и разработку планов реагирования на инциденты.

Долгосрочный репутационный ущерб

Публичное признание нарушения может нанести значительный репутационный ущерб, что потенциально может привести к долгосрочной потере доверия клиентов и снижению бизнеса. Это может иметь далеко идущие последствия для ценности бренда организации здравоохранения и ее способности привлекать и удерживать пациентов.

I. Образование/Исследования

Последствия кибератак на сектор образования и исследований в регионе серьёзны и могут иметь долгосрочные последствия для вовлеченных учреждений. Вот некоторые из ключевых эффектов:

Нарушение образовательных услуг

Кибератаки могут привести к значительным сбоям в предоставлении образовательных услуг. Поскольку многие учреждения полагаются на цифровые платформы для обучения и исследований, кибератака может остановить занятия, задержать исследовательские проекты и привести к потере данных, что повлияет на студентов, преподавателей и результаты исследований.

Компрометация конфиденциальных данных

Образовательные учреждения хранят множество конфиденциальных данных, включая личную информацию студентов и сотрудников, финансовые отчеты и данные собственных исследований. Кибератаки могут привести к краже таких данных, что приведет к нарушению конфиденциальности и потенциальной краже личных данных.

Финансовые затраты

Финансовые последствия кибератаки на образовательные учреждения могут быть существенными. Затраты могут включать в себя выкуп, восстановление и восстановление системы, усиление мер кибербезопасности, а также потенциальные судебные издержки и штрафы за утечку данных.

Ущерб репутации

Успешная кибератака может нанести ущерб репутации учебного заведения, привести к потере доверия среди учащихся, родителей и академического сообщества. Это может иметь долгосрочные последствия для числа учащихся и партнерских отношений.

Вопросы регулирования и соответствия

На образовательные учреждения распространяются различные правила, касающиеся защиты данных и конфиденциальности. Кибератаки, приводящие к утечке данных, могут привести к проблемам с несоблюдением требований, что приводит к штрафам и судебным разбирательствам.

Влияние на исследования

Кибератаки могут поставить под угрозу ценные исследования, что приведет к потере данных, краже интеллектуальной собственности и срыву исследовательской деятельности. Это может оказать существенное влияние на научный прогресс и инновации.

Увеличение затрат на кибербезопасность

В ответ на киберугрозы образовательные учреждения должны инвестировать в меры кибербезопасности, что может стать значительным экономическим бременем. Сюда входят затраты на технологии безопасности, обучение и, возможно, найм дополнительного персонала по кибербезопасности.

Утечка талантов и ресурсов

Инциденты кибербезопасности могут отвлекать внимание и ресурсы ИТ-персонала от их основных обязанностей, влияя на общую производительность и операционную эффективность учреждения.

Долгосрочное образовательное воздействие

Долгосрочное воздействие кибератак на образование может включать снижение качества образования из-за разрушения платформ цифрового обучения и потенциальную потерю исследовательских данных, на восстановление которых могут уйти годы.