Аннотация – В этом документе представлен анализ рынка кибер-страхования, на котором в последние годы наблюдался значительный рост и проблемы. Национальная страховая ассоциация (NAIC) сообщила о росте премий по кибер-страхованию на 75% в период с 2020 года по недавний период, что указывает на реакцию рынка на растущие кибер-угрозы и растущий спрос на страховое покрытие. Несмотря на этот рост, рынок является относительно новым, за последние пять-семь лет он значительно расширился и в настоящее время сталкивается с такими проблемами, как высокий спрос, превышающий готовность предложения, и неподходящая практика андеррайтинга.

Документ полезен тем, что специалисты по безопасности и специалисты из различных отраслей смогут понять последствия роста рынка кибер-страхования и полезность анализа для совершенствования мер кибербезопасности и стратегий управления рисками.

I. Текущее состояние рынка

S&P Global Ratings сообщило, что глобальные премии по кибер-страхованию достигли около 12 миллиардов долларов в 2022 году и прогнозируют среднегодовой рост на 25%–30%, потенциально достигая 23 миллиардов долларов к 2025 году. Рост рынка кибер-страхования в значительной степени зависит от перестраховочной защиты, и перестраховщики считаются решающими для его устойчивого расширения. Отрасли рекомендуется способствовать более устойчивому базовому росту, который зависит не только от повышения ставок, но и от устранения системных кибер-рисков и расширения охвата большего числа малых и средних предприятий.

Текущее состояние рынка кибер-страхования демонстрирует признаки стабилизации после периода высокого давления и роста премий. Этот рынок описывается как «сложный», поскольку страховщики сталкиваются с такими проблемами, как рост премий и снижение гибкости в плане политики. Однако последние тенденции показывают, что темпы роста страховых взносов замедляются, а в некоторых случаях продление полисов происходит по фиксированным ставкам.

Несмотря на эту стабилизацию, не ожидается, что рынок вернётся к более мягким условиям, наблюдавшимся в предыдущие годы. Продукты теперь покрывают меньше, а операторы связи вводят новые ограничительные формулировки политики. Строгие требования к контролю над андеррайтингом, которые действовали в прошлом, сохранятся, а спрос на мощности по-прежнему превышает предложение. Кроме того, на рынках кибер-страхования растёт обеспокоенность по поводу системного кибер-риска, который фокусируется на количественной оценке последствий катастрофического кибер-события.

Рынок кибер-страхования является относительно новым, набравшим значительную популярность за последние пять-семь лет, и он все ещё сталкивается с различными проблемами. Страховщики разрабатывают более строгие требования к полису, что привело к уменьшению количества страховых компаний и увеличению спроса. Тем не менее, есть оптимизм в отношении того, что страховщики и поставщики будут сотрудничать для разработки устойчивых решений с упором на улучшение управления рисками и их количественную оценку.

A. Топ кибер-инцидентов

Полисы кибер-страхования обычно покрывают целый ряд кибер-атак и инцидентов, в том числе:

- **Утечки данных.** инциденты связаны с несанкционированным доступом к конфиденциальным данным или их кражей. Кибер-страхование может помочь покрыть расходы, связанные с реагированием на утечку данных, такие как расходы на уведомление, услуги кредитного мониторинга и судебные издержки.
- **Инциденты сетевой безопасности:** сюда входят атаки, которые ставят под угрозу безопасность сети компании, например заражение вредоносным ПО, распределённые атаки типа «отказ в обслуживании» (DDoS) и другие.
- **Вымогательство.** страхование часто покрывает расходы, связанные с кибер-вымогательством, например атаки программ-вымогателей, когда хакеры требуют оплаты за восстановление доступа к цифровым активам компании.
- **Уничтожение данных.** если кибер-атака приводит к потере или уничтожению данных, кибер-страхование может помочь покрыть расходы на восстановление данных.
- **Перебои в работе компании.** если кибер-атака нарушает работу компании, кибер-страхование может покрыть потерю дохода во время простоя и затраты на восстановление операций.

- **Халатность:** данное покрытие распространяется на убытки, возникшие в результате ошибок или халатности при предоставлении услуг с учётом сбоев в услугах кибербезопасности.
- **Ответственность СМИ:** сюда входят претензии, связанные с цифровым контентом, такие как обвинения в нарушении авторских прав, клевете или вторжении в частную жизнь.

II. Страхование ответственности или кибер-страхование

Кибер-страхование и страхование кибер-ответственности — это термины, которые часто используются как синонимы, но в зависимости от контекста они могут относиться к разным типам покрытия.

Кибер-страхование — это широкий термин, который обычно относится к ряду покрытий, предназначенных для защиты бизнеса от различных рисков, связанных с технологиями. Оно может включать как собственные, так и сторонние покрытия. Страхование собственной стороны страхует от финансовых потерь, которые застрахованная организация несёт непосредственно из-за кибер-инцидента, таких как убытки от прерывания бизнеса, затраты на восстановление данных и выплаты выкупа. Страхование третьих лиц относится к страхованию ответственности за претензии, предъявленные к застрахованной организации в связи с кибер-инцидентом, например, судебные иски, связанные с утечкой данных.

С другой стороны, страхование кибер-ответственности часто используется для обозначения части страхования ответственности перед третьими лицами в полисе кибер-страхования. Он покрывает ответственность застрахованной организации за ущерб, возникший в результате утечки данных или потери конфиденциальной информации. Сюда могут входить расходы, связанные с юридической защитой, урегулированием споров и вынесением судебных решений, а также штрафы и пени, налагаемые регулирующими органами.

Оба типа полисов направлены на смягчение финансовых последствий кибер-событий, но конкретные покрытия могут сильно различаться в зависимости от страховщиков и отдельных полисов.

A. Полисы страхования кибер-ответственности

Кибер-ответственность обычно включает покрытие претензий третьих сторон, возникших в результате кибер-инцидентов:

- **Покрытие ответственности за конфиденциальность:** защищает от ответственности, возникающей в результате утечки данных, которая раскрывает частные данные, и нарушений закона о конфиденциальности.
- **Инциденты сетевой безопасности:** покрывает убытки из-за нарушений безопасности, таких как несанкционированный доступ, вредоносное ПО и DDoS-атаки.
- **Нарушение работы бизнеса:** обеспечивает покрытие потери дохода и дополнительных расходов, понесённых в результате кибер-события, которое нарушает работу бизнеса.
- **Ответственность СМИ:** охватывает юридические претензии, связанные с электронным контентом, такие как нарушение авторских прав, клевета или вторжение в частную жизнь.
- **Халатность:** защищает от потерь из-за ошибок в предоставляемых услугах, особенно для фирм, предоставляющих технологические и профессиональные услуги.

B. Полисы кибер-страхования

покрытие как собственных, так и третьих сторон. Типичные включения:

- **Уничтожение данных:** покрывает расходы, связанные с потерей или повреждением данных.
- **Вымогательство:** обеспечивает защиту от угроз раскрытия конфиденциальной информации или атак на системы, если не будет уплачен выкуп.
- **Интернет-кража:** защищает от потерь из-за несанкционированных онлайн-транзакций.
- **Хакерская деятельность:** покрывает ущерб от взлома, включая утечку данных и вторжение в систему.
- **Отказ в обслуживании:** включает покрытие убытков, вызванных преднамеренными или случайными атаками типа «отказ в обслуживании».
- **Фонды вознаграждения за преступления:** некоторые политики могут предлагать средства за информацию, ведущую к аресту и осуждению киберпреступников.

III. Текущие тенденции на рынке кибер-страхования

Современные тенденции на рынке кибер-страхования:

- **Рост рынка:** прогнозируется, что рынок кибер-страхования вырастет с 16,66 млрд долларов США в 2023 году до 84,62 млрд долларов США к 2030 году, при этом среднегодовой темп роста составит 26,1% в течение прогнозируемого периода.
- **Географическое доминирование.** Ожидается, что Северная Америка будет доминировать на рынке кибер-страхования в течение прогнозируемого периода.
- **Увеличение спроса.** Существует высокий спрос на кибер-страхование из-за растущего внедрения общедоступных облачных сервисов, развития моделей рабочего пространства, увеличения угроз кибербезопасности и потребности в технологических достижениях.

- **Стабилизация рынка.** После периода быстрого роста премий рынок начинает стабилизироваться. Это связано с тем, что страховщики совершенствуют свои методы оценки рисков, новыми участниками рынка, обеспечивающими покрытие, а также естественным балансом спроса и предложения.
- **Более строгий андеррайтинг:** страховщики разрабатывают более строгие требования к полисам, что привело к сокращению количества страховых компаний и увеличению спроса.
- **Фокус на управлении рисками.** Управление кибер-рисками становится основным направлением деятельности в цифровом мире, и кибер-страхование рассматривается как неотъемлемая часть этого процесса. Отрасль работает над созданием устойчивого рынка кибер-страхования.
- **Влияние технологических тенденций.** Ожидается, что будущие кибер-атаки будут ускоряться благодаря ключевым технологическим тенденциям, таким как искусственный интеллект, мета-вселенная и конвергенция ИТ, Интернета вещей и операционных технологий (ОТ), которые создадут новые поверхности для атак и системные риски.
- **Нормализация цен.** Рост цен на кибер-страхование прекратился в четвёртом квартале 2022 года, что указывает на тенденцию к нормализации цен.
- **Увеличение удержаний по самострахованию.** Удержания по самострахованию продолжают увеличиваться, а это означает, что застрахованные стороны сохраняют больше риска до того, как начнёт действовать страховое покрытие.
- **Изменения основных лимитов:** снижение основных лимитов, которое было тенденцией, прекратилось в течение 2022 года.

IV. Изменения рынка за последний год

Рынок кибер-страхования претерпел значительные изменения за последний год, с 2023 по 2024 год. Вот некоторые ключевые изменения:

- **Нормализация рынка.** После двух лет роста цен рынок кибер-страхования нормализуется. Коэффициенты убытков страховых компаний сейчас лучше, чем в последние несколько лет.
- **Рост цен прекратился:** рост цен на кибер-страхование прекратился в четвёртом квартале 2022 года.
- **Продолжающееся внимание к средствам контроля безопасности.** Андеррайтеры продолжают уделять внимание мерам безопасности, которые представляют собой меры, принимаемые для защиты цифровых активов.
- **Стабилизация.** Рынок кибер-страхования начал стабилизироваться после всплеска атак программ-вымогателей в последние годы.
- **Снижение цен.** Цены на кибер-страхование в США продолжали снижаться, снизившись на 6% в третьем квартале 2023 года.

V. Изменения страховых премий за последний год

За последний год на рынке кибер-страхования произошло несколько изменений в размерах премий:

- **Увеличение прямых письменных премий:** Прямые письменные премии по отдельному страхованию кибербезопасности в 2022 году увеличились на 61,5% по сравнению с предыдущим годом.
- **Стабилизация цен.** На рынке началась некоторая коррекция в 2022 и 2023 годах, когда цены на кибер-страхование начали стабилизироваться. Прямые письменные премии на признанном рынке выросли примерно на 50% в 2022 году по сравнению с увеличением более чем на 75% в 2021 году.
- **Снижение темпов роста политики:** количество действующих политик сократилось на 6,8% в 2021 году, но увеличилось на 4,4% в 2022 году.
- **Одобрения и исключения:** страховщики внедряют одобрения в отношении мер безопасности, чтобы ограничить свои риски и ужесточить формулировки политики, ограничивая покрытие путём исключений.
- **Повышенная ответственность за кибер-гигиену**: страхователям приходится более ответственно относиться к своей кибер-гигиене при получении страхового покрытия, а процесс подачи заявления стал более сложным.
- **Умеренный рост ставок:** цены на кибер-страхование в США выросли в среднем на 11% в годовом исчислении в первом квартале 2023 года, что было меньшим увеличением по сравнению с ростом на 28% в четвёртом квартале 2022 года. Темпы роста были умеренными, со средним ростом на 17% в декабре 2022 года по сравнению с высоким средним ростом в 133% в декабре 2021 года.
- **Снижение цен.** Цены на кибер-страхование в США продолжали снижаться, снизившись на 6% в третьем квартале 2023 года.

Эти изменения указывают на то, что рынок переживает переход от быстрого роста премий к более стабильному и умеренному росту премий, при этом страховщики становятся более избирательными и осторожными в своей практике андеррайтинга.

VI. Повышенный спрос

К наиболее распространённым типам кибер-атак, которые привели к увеличению спроса на кибер-страхование в прошлом году, относятся:

- **Атаки программ-вымогателей.** Число атак программ-вымогателей резко возросло, что привело к значительному увеличению претензий по кибер-страхованию. В этих атаках киберпреступники шифруют данные жертвы и требуют выкуп за их раскрытие. Средний спрос на выкуп также увеличился, что ещё больше стимулирует спрос на кибер-страхование.
- **Утечки данных.** Утечки данных остаются серьёзной проблемой, поскольку все больше страховых клиентов выбирают киберзащиту. Эти нарушения связаны с несанкционированным доступом к конфиденциальным данным, что может привести к значительному финансовому и репутационному ущербу.
- **Кибер-атаки на кибер-физические системы.** Атаки на кибер-физические системы, предполагающие взаимодействие цифровых и физических компонентов, растут. По оценкам, ущерб от этих атак достигнет более 50 миллиардов долларов США, что подчёркивает растущий риск и необходимость кибер-страхования.
- **Крупномасштабные атаки.** Крупномасштабные атаки, такие как атака с использованием программы-вымогателя Colonial Pipeline, выявили потенциал значительных сбоев и финансовых потерь, что увеличивает спрос на кибер-страхование.

VII. Страхование и отрасли

Премии по кибер-страхованию могут значительно различаться в зависимости от отрасли и размера компании

- **Факторы отраслевого риска:** некоторые отрасли считаются более рискованными из-за характера их деятельности и данных, которые они обрабатывают. Например, отрасли здравоохранения, финансов и розничной торговли часто обрабатывают конфиденциальные данные клиентов, что делает их привлекательными целями для киберпреступников. В результате компании в этих отраслях могут столкнуться с более высокими премиями.
- **Размер компании.** Более крупные компании обычно имеют более сложные системы и больше данных, что может увеличить их профиль риска. Поэтому им могут грозить более высокие премии. Однако малые и средние предприятия с сильным кибер-контролем и в отраслях с низким уровнем риска могут иметь средние премии в диапазоне от примерно 1400 до примерно 3000 долларов за миллион лимита.
- **Средства контроля кибербезопасности.** Компании с надёжным контролем и практикой кибербезопасности могут рассматриваться как менее рискованные и, следовательно, могут получить выгоду от более низких премий. И наоборот, компании, не имеющие базового контроля кибер-гигиены, могут столкнуться с более высокими страховыми взносами или даже столкнуться с трудностями при получении страхового покрытия.
- **История претензий.** Компании, в истории которых происходили кибер-инциденты, могут рассматриваться как компании с более высоким риском и получать более высокие премии.
- **Потребности в страховом покрытии.** Конкретные потребности компании в страховом покрытии, такие как тип и размер страхового покрытия, также могут влиять на размер премии. Более полное покрытие обычно предполагает более высокие страховые взносы.

VIII. Проблемы страхового рынка

В прошлом году рынок кибер-страхования столкнулся с рядом проблем:

- **Недостаток исторических данных.** Индустрия кибер-страхования сталкивается с нехваткой исторических данных, что затрудняет прогнозирование будущих кибер-рисков и установление цен на кибер-страхование.
- **Высокий спрос, ограниченное предложение.** Спрос на кибер-страхование растёт, но ограниченные возможности со стороны предложения привели к росту ставок и корректировкам покрытия, сроков и условий.
- **Просчёт риска.** Рынок кибер-страхования понёс значительные потери из-за просчёта риска, что привело к переходу рынка от мягкого цикла, характеризующегося более низкими премиями и более высокими лимитами, к жёсткому циклу, что привело к стремительному росту страховых премий.
- **Неподходящая практика андеррайтинга.** Рынок характеризуется неподходящей практикой андеррайтинга, при этом страховщики разрабатывают более строгие требования к полисам, что приводит к сокращению числа страховых компаний и резкому росту спроса.
- **Системный кибер-риск:** возможность крупномасштабной атаки, при которой потери сильно коррелируют между компаниями, затрудняет разработку комплексной политики.

- **Проблемы, специфичные для сектора.** Определённые сектора с исторически плохим состоянием безопасности, такие как образование, или узкоспециализированные сектора, такие как разработчики программного обеспечения, могут испытывать более трудные времена с получением покрытия.

IX. РАЗНИЦА СТРАХОВЫХ ВЗНОСОВ

Премии по кибер-страхованию могут значительно различаться в зависимости от отраслей с высокими и низкими кибер-рисками.

Для отраслей с высокими кибер-рисками, таких как здравоохранение, финансы и розничная торговля, которые часто обрабатывают конфиденциальные данные клиентов, премии обычно выше. Эти отрасли являются привлекательными целями для киберпреступников, и в результате они сталкиваются с более высокими премиями из-за повышенного риска.

С другой стороны, в отраслях с низкими кибер-рисками, например в отраслях со строгим кибер-контролем, средние премии могут варьироваться от примерно 1400 до примерно 3000 долларов за миллион лимита.

Кроме того, размер компании также играет роль в стоимости премии. Более крупные компании обычно имеют более сложные системы и больше данных, что может увеличить их профиль риска и, следовательно, они могут столкнуться с более высокими премиями. И наоборот, более мелкие предприятия в отраслях с низким уровнем риска и строгим кибер-контролем могут иметь более низкие премии.

Страховщики также стали более избирательно подходить к тому, кто и что покрывается страховкой, и ужесточили условия полиса, чтобы сократить непредвиденные убытки.

Высокие премии на рынке кибер-страхования обусловлены несколькими факторами:

- **Рост кибер-угроз.** Число и стоимость кибер-угроз растут, что, в свою очередь, увеличивает стоимость страховых премий. По мере роста стоимости угроз растёт и стоимость премий.
- **Рост претензий.** Частота и стоимость претензий растут, что приводит к увеличению коэффициента убытков страховщиков. Это привело к увеличению премий для покрытия возросших выплат.
- **Недостаток исторических данных.** На рынке кибер-страхования отсутствуют обширные исторические данные, что затрудняет страховщикам точное прогнозирование будущих рисков и соответствующее установление премий.
- **Отраслевые риски:** риск и, следовательно, стоимость кибер-страхования могут значительно различаться в зависимости от отрасли. Отрасли с более высокими кибер-рисками обычно сталкиваются с более высокими премиями.
- **Размер и характер бизнеса.** Размер и характер бизнеса также могут влиять на размер страховых премий. Более крупные предприятия или предприятия с более высоким профилем риска обычно сталкиваются с более высокими премиями.
- **Географическое положение и нормативно-правовая среда.** Местоположение предприятия и нормативно-правовая среда, в которой оно работает, также могут влиять на премии. Например, предприятия, работающие в регионах со строгими правилами защиты данных, могут столкнуться с более высокими премиями.
- **Тип покрытия.** Тип покрытия, который выбирает компания, также может влиять на размер страховых взносов. Более полное покрытие обычно сопровождается более высокими страховыми взносами.
- **Практика управления рисками.** Страховщики часто учитывают практику кибербезопасности компании при установлении премий. Компании, применяющие надёжные меры кибербезопасности, могут быть вознаграждены более низкими премиями, в то время как компании с плохой практикой могут столкнуться с более высокими премиями.

X. СТРАХОВОЕ ПОКРЫТИЕ

Полисы кибер-страхования обычно покрывают широкий спектр кибер-атак, а конкретное покрытие может варьироваться в зависимости от размера бизнеса и конкретных рисков, с которыми он сталкивается:

- **Утечки данных:** это один из наиболее распространённых типов кибер-атак, покрываемых кибер-страхованием. Речь идёт об инцидентах, когда к конфиденциальным, защищённым или конфиденциальным данным был получен доступ или они были раскрыты несанкционированным образом.
- **Кибер-вымогательство:** сюда входят атаки программ-вымогателей, когда тип вредоносного программного обеспечения угрожает опубликовать данные жертвы или навсегда заблокировать доступ к ним, если не будет уплачен выкуп.
- **Нарушения сетевой безопасности:** сюда относятся инциденты, когда неавторизованное лицо получает доступ к сети компании, что потенциально может привести к краже или повреждению данных.

- **Перебои в бизнесе:** сюда входят убытки, которые бизнес может понести из-за кибер-атаки, нарушающей его нормальную бизнес-операцию.
- **Ответственность за конфиденциальность:** сюда входят обязательства, возникающие в результате нарушений закона о конфиденциальности или кибер-инцидентов, в результате которых раскрываются частные данные.

Для крупных корпораций эти полисы часто включают покрытие обязательств перед третьими лицами, таких как расходы, связанные со спорами или судебными исками, убытки, связанные с клеветой, а также нарушением авторских прав или товарных знаков.

Для малых предприятий страховое покрытие может быть в большей степени сосредоточено на убытках, таких как расходы, связанные с уведомлением клиентов о взломе, оплатой судебных издержек и наймом экспертов по компьютерной криминалистике для восстановления скомпрометированных данных.

Предприятиям часто требуется сочетание как собственных, так и сторонних страховок, чтобы быть полностью защищёнными от целого ряда кибер-рисков, с которыми они сталкиваются.

A. *Собственное страхование в полисах кибер-страхования*

Страхование предназначено для покрытия прямых расходов, которые бизнес несёт в результате кибер-инцидента:

- **Прерывание деятельности:** потеря дохода и дополнительные расходы, понесённые из-за кибер-события, которое нарушает деятельность бизнеса.
- **Кибер-вымогательство:** покрытие выплат выкупа, произведённых в ответ на программы-вымогатели или другие угрозы кибер-вымогательства.
- **Восстановление данных:** Затраты, связанные с восстановлением или заменой утерянных или повреждённых данных.
- **Затраты на уведомление:** расходы на уведомление пострадавших лиц, клиентов или регулирующих органов после утечки данных.
- **Услуги кредитного мониторинга:** затраты на услуги кредитного мониторинга, предлагаемые пострадавшим лицам после утечки данных.
- **Связи с общественностью:** расходы, связанные с управлением репутацией компании после кибер-инцидента.
- **Судебное расследование:** гонорары экспертам за определение причины и масштаба кибер-нарушения.

B. *Страхование третьих лиц в полисах кибер-страхования*

Страхование ответственности третьих лиц — это страхование ответственности, которое защищает бизнес от претензий других лиц (клиентов, партнёров и т. д.) в связи с кибер-инцидентом, за который компания несёт ответственность. Это покрытие обычно включает в себя:

- **Расходы на юридическую защиту:** Плата за защиту от судебных исков, связанных с кибер-инцидентами.
- **Мировые соглашения и судебные решения:** расходы на судебные приговоры или урегулирования, возникающие в результате таких исков.
- **Нормативные штрафы и пени:** покрытие штрафов и санкций, которые могут быть наложены регулирующими органами после утечки данных или кибер-инцидента.
- **Ответственность перед СМИ:** защита от претензий о нарушении прав интеллектуальной собственности, клевете или вторжении в частную жизнь из-за электронного контента.

C. *Чем отличаются полисы кибер-страхования от третьих сторон по размеру премий?*

Размер страховых взносов по полисам кибер-страхования, предоставляемым собственными и третьими сторонами, может варьироваться в зависимости от нескольких факторов, и разница между ними обычно не стандартизируется в отрасли.

При страховании на размер страховых взносов часто влияют тип и объём конфиденциальных данных, которыми владеет компания, её отрасль, надёжность мер кибербезопасности и история кибер-инцидентов. Чем обширнее потенциальные прямые затраты (например, прерывание деятельности, восстановление данных и антикризисное управление), тем выше, вероятно, будет премия.

С другой стороны, премии по страхованию третьих лиц часто зависят от подверженности компании рискам ответственности. Это может зависеть от таких факторов, как характер деятельности компании, степень, в которой она обрабатывает или имеет доступ к данным третьих сторон, а также её договорные обязательства, связанные с безопасностью данных. Компании, которые предоставляют технологические услуги или обрабатывают большие объёмы сторонних данных, могут столкнуться с более высокими премиями за стороннее покрытие.

Важно отметить, что многие полисы кибер-страхования включают покрытие как собственных, так и третьих сторон,

и общая премия по такому полису будет отражать совокупный риск. Как и в случае любого другого страхования, премии могут сильно различаться между страховщиками и отдельными полисами, поэтому предприятиям следует получать котировки от нескольких страховщиков, чтобы гарантировать, что они получают наилучшую стоимость.

D. Чем отличаются полисы кибер-страхования от третьих лиц с точки зрения франшизы

Франшизы по полисам кибер-страхования как для собственной, так и для третьей стороны могут варьироваться в зависимости от нескольких факторов, включая тип и размер бизнеса, уровень кибер-риска, с которым он сталкивается, а также конкретные покрытия, включённые в полис.

При страховании на франшизу могут влиять потенциальные прямые затраты бизнеса в результате кибер-инцидента, такие как прерывание деятельности, восстановление данных и затраты на антикризисное управление. Компания с надёжной инфраструктурой кибербезопасности и хорошим опытом управления кибер-рисками может договориться о более низкой франшизе.

При страховании третьих лиц на франшизу может влиять подверженность бизнеса рискам ответственности. Компании, которые обрабатывают большое количество сторонних данных или предоставляют технологические услуги, могут иметь более высокие франшизы из-за повышенного риска претензий третьих сторон.

Как правило, более высокие франшизы приводят к более низким страховым взносам, и наоборот. Таким образом, предприятия должны сбалансировать стремление к более низким страховым взносам с возможностью платить более высокую франшизу в случае претензии.

E. Факторы, влияющие на премии по собственным полисам кибер-страхования

На размер страховых взносов по полисам кибер-страхования могут повлиять несколько факторов:

- **Тип и объём данных.** Компании, которые обрабатывают большие объёмы конфиденциальных данных, таких как личная информация или данные кредитных карт, могут столкнуться с более высокими премиями из-за повышенного риска утечки данных.
- **Отрасль:** некоторые отрасли, такие как здравоохранение и финансы, часто становятся объектами атак киберпреступников и могут столкнуться с более высокими премиями.
- **Меры кибербезопасности.** Компании, применяющие надёжные меры кибербезопасности, могут договориться о более низких страховых взносах.
- **Прошлые инциденты:** Компании, в прошлом сталкивавшиеся с кибер-инцидентами, могут столкнуться с более высокими премиями.
- **Доход:** более крупные компании с более высокими доходами могут столкнуться с более высокими страховыми премиями из-за более серьёзных потенциальных финансовых последствий кибер-инцидента.
- **Пределы покрытия и франшизы:** более высокие лимиты покрытия и более низкие франшизы обычно приводят к более высоким страховым взносам.

F. Факторы, влияющие на премии по сторонним полисам кибер-страхования

На размер премий по полисам кибер-страхования третьих лиц также могут влиять несколько факторов:

- **Тип предоставляемых услуг:** Компании, предоставляющие услуги, связанные с доступом к сторонним данным или системам, могут столкнуться с более высокими премиями из-за повышенного риска ответственности.
- **Контрактные обязательства:** Компании могут столкнуться с более высокими премиями, если у них есть контрактные обязательства, которые увеличивают их ответственность в случае утечки данных.
- **Отрасль:** как и в случае с собственным страхованием, некоторые отрасли могут столкнуться с более высокими страховыми премиями из-за повышенного риска кибер-инцидентов.
- **Прошлые инциденты:** история кибер-инцидентов или претензий может привести к более высоким выплатам.
- **Пределы покрытия и франшизы.** Как и в случае с собственным страхованием, более высокие лимиты покрытия и более низкие франшизы обычно приводят к более высоким страховым взносам.

XI. Исключения из страхования

Полисы кибер-страхования обычно включают в себя несколько исключений, которые представляют собой конкретные ситуации или обстоятельства, не подпадающие под действие полиса.:

- **Война и терроризм.** Полисы кибер-страхования обычно не включают покрытие убытков, возникших в результате военных действий, терроризма или других враждебных действий.
- **Физический ущерб:** если кибер-атака разрушает физическую инфраструктуру или оборудование, страховщик не может покрыть расходы на ремонт или замену этих активов.
- **Технологические улучшения:** Кибер-страхование помогает предприятиям восстановить свои компьютерные системы до состояния, в котором они находились до кибер-инцидента. Однако стоимость модернизации или усовершенствования технологии обычно не покрывается.

- **Незашифрованные данные:** если утечка данных связана с незашифрованными данными, страховщик может отклонить иск на основании этого исключения. Чтобы свести к минимуму риск отклонения претензии, предприятиям следует следовать лучшим отраслевым практикам шифрования данных и других мер безопасности.
- **Потенциальная будущая упущенная выгода и потеря стоимости из-за кражи интеллектуальной собственности.** Полисы кибер-страхования обычно не покрывают потенциальную будущую упущенную выгоду или потерю стоимости из-за кражи интеллектуальной собственности.

XII. Отрасли с высоким кибер-риском

Отраслями с высоким уровнем кибер-риска обычно являются те, которые обрабатывают конфиденциальные данные и имеют высокую степень цифровой связи:

- **Здравоохранение:** эта отрасль является основной мишенью из-за конфиденциального характера данных, которые она обрабатывает, включая личную медицинскую информацию и платёжные реквизиты. Кибер-атаки также могут нарушить работу критически важных служб здравоохранения.
- **Финансовые услуги.** Банки и другие финансовые учреждения являются привлекательными целями из-за финансовых данных, которые они обрабатывают. Они часто преследуются с целью получения финансовой выгоды или разрушения финансовых систем.
- **Образование:** Образовательные учреждения часто располагают большими объёмами персональных данных и исследовательской информации, что делает их привлекательными целями. Они также часто имеют менее надёжные меры кибербезопасности по сравнению с другими секторами.
- **Розничная торговля.** Розничные торговцы обрабатывают большой объём личных и финансовых данных клиентов, что делает их привлекательными целями для киберпреступников. Платформы электронной коммерции особенно уязвимы из-за своей онлайновой природы.
- **Государственный сектор:** правительственные учреждения часто подвергаются нападениям из-за хранимой ими конфиденциальной информации, которая может включать личные данные, финансовую информацию и государственную тайну. Эти атаки могут быть мотивированы финансовой выгодой, шпионажем или подрывом деятельности.
- **Производство:** Производственный сектор становится все более объектом нападений из-за его высокого фактора разрушения и возможности кражи интеллектуальной собственности.
- **Автомобильная промышленность.** Автомобильная промышленность становится мишенью из-за растущего числа транспортных средств и возможности крупномасштабных сбоев.

XIII. Отрасли с низким кибер-риском

Низко-рисковые отрасли включают в себя:

- **Сельское хозяйство.** Традиционное сельское хозяйство может быть не столь привлекательным для киберпреступников из-за меньшей зависимости от цифровых технологий и меньшего количества ценных цифровых активов по сравнению с другими отраслями.
- **Строительство.** Хотя строительные компании все чаще используют технологии, они могут быть не столь ценными объектами, как такие отрасли, как финансы или здравоохранение.
- **Развлечения и средства массовой информации.** Хотя эти отрасли действительно сталкиваются с кибер-рисками, особенно связанными с кражей интеллектуальной собственности, они, возможно, не так сильно подвергаются воздействию конфиденциальных персональных данных, как такие отрасли, как здравоохранение или финансовые услуги.
- **Услуги (нефинансовые):** Сферы услуг, которые не обрабатывают большие объёмы конфиденциальных финансовых данных, могут столкнуться с меньшими кибер-рисками.

Важно отметить, что ни одна отрасль не застрахована от кибер-рисков, а уровень риска может варьироваться внутри отрасли в зависимости от конкретной практики компании и её подверженности. Даже в отраслях, в которых обычно считается более низкий кибер-риск, компании, которые больше связаны с цифровыми технологиями или обрабатывают любые конфиденциальные данные, все равно могут сталкиваться со значительными рисками и должны принимать соответствующие меры кибербезопасности.

XIV. Отраслевые кибер-риски

.

Здравоохранение

- **Утечки данных.** Медицинские организации хранят большие объёмы конфиденциальных данных, что делает их главной мишенью для утечек данных.
- **Программы-вымогатели.** Киберпреступники нацелены на здравоохранение, чтобы вызвать сбои в работе и вымогать деньги, шифруя данные пациентов и требуя выкуп.

Финансовые услуги

- **Кража данных.** Финансовые учреждения преследуются из-за финансовых данных, которые они обрабатывают, и которые могут быть использованы для мошенничества или проданы в даркнете.
- **Нарушение системы.** Атаки, направленные на нарушение работы финансовых систем, могут иметь широкомасштабные экономические последствия.

Образование

- **Утечки данных.** Образовательные учреждения хранят ценные исследовательские данные и личную информацию студентов и сотрудников, которые могут быть атакованы.
- **Программы-вымогатели.** Школы и университеты все чаще становятся жертвами атак программ-вымогателей, которые нарушают работу и получают доступ к конфиденциальным данным.

Розничная торговля

- **Мошенничество с платёжными картами.** Розничные торговцы обрабатывают большие объёмы платёжных транзакций, что делает их мишенью для киберпреступников, стремящихся украсть информацию о кредитных картах.
- **Атаки на электронную коммерцию.** Платформы онлайн-торговли подвержены различным кибер-атакам, включая утечку данных и атаки типа «отказ в обслуживании».

Государственный сектор

- **Шпионаж.** Правительственные данные часто крадут в шпионских целях.
- **Финансовая выгода:** Государственное управление нацелено на получение финансовой выгоды посредством различных кибер-атак.

Производство

- **Кража интеллектуальной собственности.** Производственные компании становятся жертвами хакеров, которые хотят украсть интеллектуальную собственность, такую как дизайн продукции и чертежи.
- **Нарушение работы.** Кибер-атаки могут привести к физическому повреждению продуктов или машин, что приведёт к сбоям в работе.

Автомобильная промышленность

- **Атаки на подключённые транспортные средства.** Поскольку транспортные средства становятся все более подключёнными, они подвергаются риску кибер-атак, которые могут поставить под угрозу функциональность и безопасность транспортных средств.
- **Кража интеллектуальной собственности.** Автомобильные компании могут столкнуться с кибер-рисками, связанными с кражей проектных и производственных данных.

Сельское хозяйство

- **Кража данных.** Поскольку сельское хозяйство становится все более цифровым, данные, связанные с урожайностью сельскохозяйственных культур, здоровьем скота и производительностью техники, могут стать целью.
- **Нарушение операционной деятельности:** Кибер-атаки на сельскохозяйственные технологии могут нарушить работу сельского хозяйства.

Строительство

- **Утечки данных.** Строительные компании часто обрабатывают конфиденциальные данные проектов, которые могут стать целью киберпреступников.
- **Нарушение операционной деятельности:** Кибер-атаки на строительные технологии могут нарушить сроки реализации проекта и привести к финансовым потерям.

Развлечения и СМИ

- **Кража интеллектуальной собственности:** развлекательные и медиакомпании часто владеют ценной интеллектуальной собственностью, которая может стать целью киберпреступников.
- **Утечки данных.** Эти компании часто обрабатывают персональные данные клиентов, которые могут быть атакованы.

Услуги (нефинансовые)

- **Утечки данных.** Сервисные компании часто обрабатывают персональные данные клиентов, которые могут быть атакованы.
- **Финансовое мошенничество.** Киберпреступники могут атаковать эти компании с целью получения финансовой выгоды, например, посредством мошеннических транзакций.

XV. Прогнозы на будущее рынка кибер-страхования

Ожидается, что в рынок кибер-страхования будет иметь значительный рост, обусловленный увеличением частоты и стоимости кибер-угроз:

- **Рост рынка:** прогнозируется, что мировой рынок кибер-страхования значительно

вырастет. По данным Fortune Business Insights, в 2022 году рынок оценивался в 13,33 млрд долларов США, и, по прогнозам, к 2030 году он вырастет до 84,62 млрд долларов США, при этом среднегодовой темп роста составит 26,1% в течение прогнозируемого периода.

- **Растущий спрос.** Спрос на кибер-страхование растёт, но ограниченные возможности предложения привели к корректировкам покрытия, сроков и условий. Этот спрос, вероятно, будет продолжать расти по мере роста кибер-угроз.
- **Динамический андеррайтинг.** Поскольку управление кибер-рисками и их количественная оценка становятся все более популярными, переход к динамическому андеррайтингу станет более осуществимым. Это предполагает корректировку страховыми премиями на основе текущего состояния и практики компании в области кибербезопасности, а не статических факторов.
- **Более строгие требования:** страховщики разрабатывают более строгие требования к полисам, что может привести к уменьшению количества страховых компаний, но увеличению спроса на кибер-страхование.
- **Политики, основанные на данных:** использование данных для реализации политики будет увеличиваться. Это может привести к более точному определению премий, снижению коэффициента убыточности и повышению прибыльности страховой отрасли.
- **Расширение сотрудничества:** ожидается, что страховщики и поставщики будут более тесно сотрудничать для разработки устойчивых решений для рынка кибер-страхования. Это может включать в себя усиление коммуникации и сотрудничества для предотвращения атак.

XVI. Факторы роста

Несколько ключевых факторов способствуют росту рынка кибер-страхования:

- **Рост кибер-угроз.** Рост числа кибер-атак и утечек данных привёл к повышению осведомлённости о рисках и необходимости защиты, что привело к увеличению спроса на кибер-страхование.
- **Растущая осведомлённость:** все больше предприятий понимают необходимость кибер-страхования, поскольку они все больше осознают потенциальный финансовый и репутационный ущерб, который может возникнуть в результате кибер-угроз.
- **Нормативно-правовая среда:** Нормативно-правовая среда также является движущей силой роста. Поскольку правила защиты данных становятся более строгими, предприятия все чаще обращаются за кибер-страхованием, чтобы помочь управлять своими регуляторными рисками.
- **Цифровая трансформация.** Сдвиг бизнес-моделей в сторону большего количества возможностей цифровой и электронной коммерции увеличил подверженность кибер-угрозам, что привело к увеличению спроса на кибер-страхование.
- **Политики, основанные на данных.** Использование данных для реализации политики становится все более распространённым. Это позволяет компаниям кибер-страхования предлагать более точно оценённые премии, что может привести к снижению коэффициента убытков и повышению прибыльности отрасли, тем самым стимулируя рост.
- **Ограниченное предложение:** спрос на кибер-страхование растёт, но ограниченные возможности со стороны предложения привели к корректировкам покрытия, условий и положений, что способствовало бы росту рынка.
- **Осведомлённость о рисках и готовность:** повышение осведомлённости предприятий о кибер-рисках и признание необходимости защищать себя от этих рисков способствуют росту рынка.
- **Достижения в моделях андеррайтинга и оценки рисков:** страховщики работают над лучшим пониманием и количественной оценкой кибер-рисков, что способствует росту рынка.

Ожидается, что новые технологии будут определять будущее кибер-страхования несколькими способами:

- **ИИ и Метавселенная:** Будущие кибер-атаки будут все больше зависеть от ключевых технологических тенденций, таких как искусственный интеллект и так называемая «метавселенная».
- **Интернет вещей (IoT) и операционные технологии (OT):** Расширяющиеся миры IoT и OT открывают большие возможности, но также создают новые поверхности для атак, уязвимости и системные риски.
- **Услуги крипто-страхования:** ожидается, что растущее распространение услуг крипто-страхования будет способствовать расширению рынка, отражая растущую оцифровку финансовых услуг.

XVII. Как страховые компании адаптируются к меняющемуся киберпространству

Страховые компании адаптируются к меняющемуся киберпространству с помощью нескольких стратегий:

- **Более строгие практики андеррайтинга:** страховщики требуют более подробной информации об ИТ-системах и средствах контроля безопасности от компаний, желающих получить страховое покрытие. Это помогает им лучше оценить риск и соответствующим образом адаптировать политику.
- **Более высокие франшизы и ограничения покрытия.** Чтобы управлять рисками, страховщики увеличивают франшизы и устанавливают ограничения на покрытие, особенно в отношении системных рисков, а также технологических ошибок и упущений.
- **Акцент на упреждающем управлении рисками.** Страховщики уделяют больше внимания упреждающему управлению рисками, поощряя предприятия к использованию комплексных методов управления рисками, включая партнёрство со сторонними поставщиками услуг безопасности для выявления и устранения уязвимостей.
- **Сотрудничество с ИБ-фирмами:** страховщики сотрудничают с фирмами по кибербезопасности для разработки комплексных страховых продуктов, которые отражают лучшее понимание связанных с этим рисков.
- **Инвестиции в меры кибербезопасности:** страховщики инвестируют в надёжные меры кибербезопасности, регулярно обновляя свои системы и проводя комплексное обучение сотрудников по выявлению потенциальных угроз и реагированию на них.
- **Адаптация страховых продуктов:** Страховщики адаптируют свои продукты для удовлетворения индивидуальных потребностей клиентов, осознавая, что разные предприятия имеют разные проблемы и профили рисков.
- **Построение партнёрских отношений за пределами страховой отрасли.** Страховщики работают с государственными учреждениями, научными учреждениями и отраслевыми ассоциациями, чтобы справляться с возникающими рисками и развивать более полное понимание ландшафта кибер-угроз.
- **Адаптация к волатильности рынка.** Опытные страховщики используют свои исторические знания, чтобы ориентироваться в колебаниях рынка и предоставлять клиентам стабильные и эффективные решения.

XVIII. Страховые выплаты

Кибер-страхование имеет ряд преимуществ для бизнеса:

- **Покрытие от утечек данных.** Кибер-страхование может покрыть расходы, связанные с утечкой данных, включая судебные разбирательства, восстановление и кражу личных данных. Это особенно выгодно, учитывая, что кибер-атака в среднем может стоить компании более 1 миллиона долларов.
- **Возмещение потерь бизнеса.** атаки часто прерывают бизнес и приводят к потере доходов, что возмещается полисом.
- **Защита от кибер-вымогательства.** страхование обеспечивает защиту от вымогательства, когда критически важные бизнес-данные шифруются до тех пор, пока компания не заплатит.
- **Покрытие убытков от перерыва в бизнесе.** Кибер-страхование может покрыть убытки от перерыва в бизнесе, поддерживая бизнес на плаву в финансовом отношении, пока предпринимаются усилия по восстановлению.
- **Соответствие нормативным требованиям.** Кибер-страхование может помочь покрыть потенциальные штрафы и расходы на юридическую защиту, связанные с несоблюдением правил защиты данных.
- **Управление репутацией:** если информация о клиентах взломана или данные взяты в заложники, это может существенно повредить репутации организации. Кибер-страхование часто обеспечивает кризисное управление и поддержку по связям с общественностью для управления такими ситуациями.
- **Ресурсы для снижения рисков и восстановления:** Кибер-страхование предоставляет ресурсы для снижения рисков и восстановления, помогая предприятиям быстро реагировать на инциденты.
- **Ограничение финансовой ответственности:** страхование ограничивает финансовую ответственность бизнеса в случае кибер-атаки, предоставляя финансовую компенсацию для реагирования.
- **«Душевное спокойствие»:** страхование даёт уверенность, что предприятия приняли меры для обеспечения своей финансовой стабильности в случае кибер-инцидента.
- **Конкурентная дифференциация.** Наличие страхования может обеспечить конкурентное преимущество, демонстрируя приверженность бизнеса управлению кибер-рисками.