Страховые механизмы защиты от утечки персональных данных

16 октября 2024 года

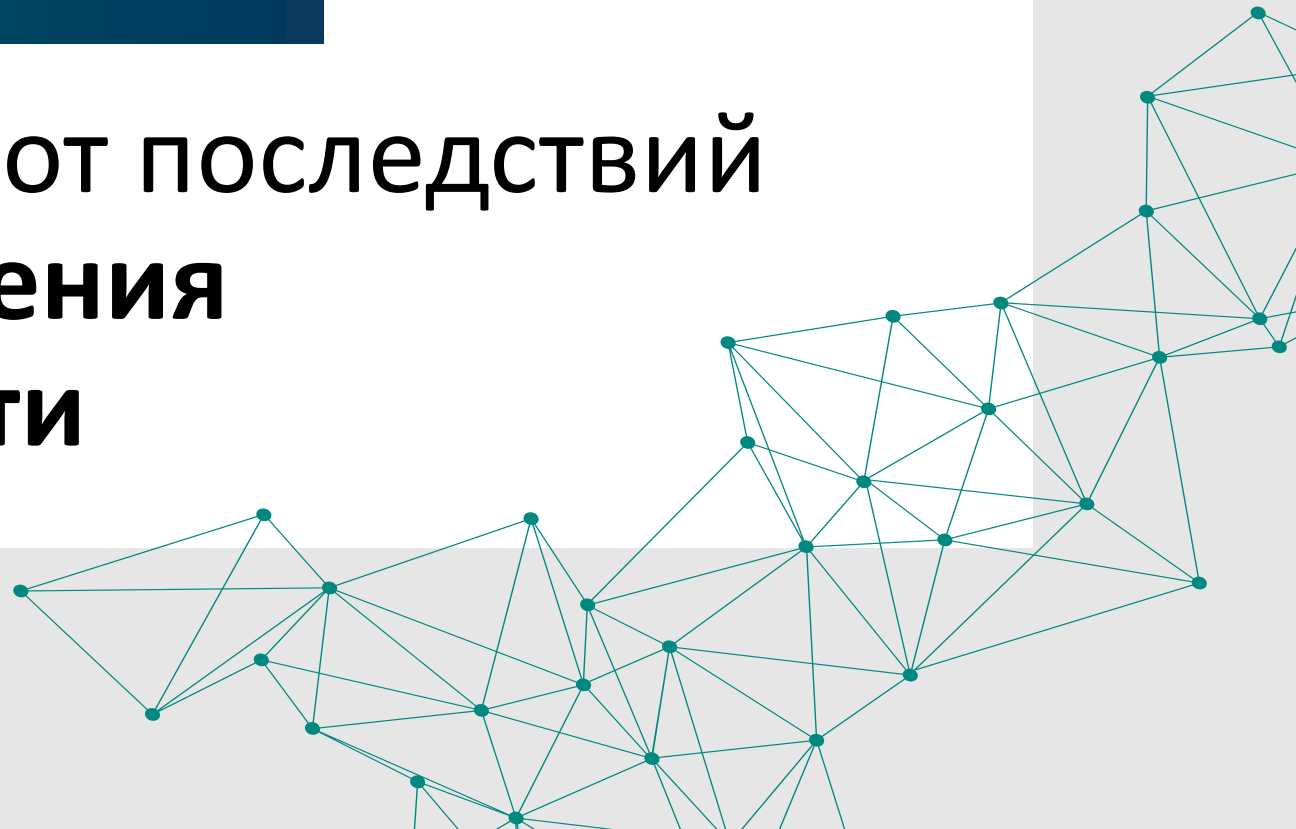
Владимир Новиков

- Управляющий директор - Директор по рискам Сбербанк страхование
- Руководитель рабочей группы Всероссийского союза страховщиков по развитию киберстрахования
- Председатель Правления Гильдии Актуариев
- Преподаватель НИУ Высшая школа экономики

01

Киберстрахование

– это страхование от последствий инцидента **нарушения кибербезопасности**



Киберинцидент

это - реализованная угроза в киберпространстве, непредвиденное событие, вызвавшее полную или частичную недоступность информационной системы и нарушающее бизнес-процесс вследствие:

- шифрования данных, блокировки или создания помех в работе информационной системе или браузеров программой-вымогателем;
- нарушения работоспособности информационной системы, вызванного вредоносным программным обеспечением;
- DoS/DDoS-атак;
- APT-атак (целевых атак);
- атак на уязвимости (нулевого дня) в системном ПО;
- подключения компьютера к ботнету вследствие заражения системы вирусом через уязвимость ПО, невнимательности пользователя (маскировка под «полезное содержимое»), использование санкционированного доступа к компьютеру.
- Kill Chain («убийственной цепочки») и т.д.

Последствия киберинцидента

01 Технические

02 Финансовые

!

В страховании последствия должны быть **финансовыми**,
так как страхование – это **компенсация финансовых потерь**

Финансовые последствия

Страхование собственных потерь

- Утрата IT систем, данных
- Расходы на перерыв в производстве
- Расходы на расследования
- Прочие расходы (восстановление репутации)

Страхование ответственности

- Ущерб жизни, здоровью, имуществу третьих лиц
- Утечка персональных данных
- Ущерб окружающей среде

Не могут быть застрахованы, запрещено законодательством РФ

- Неисполнение договора
- Штрафы, накладываемые государственными / контролирующими органами

02

Современный рынок страхования киберрисков в России и в мире

Мировой рынок

Драйвером роста страхования является законодательство

- Основные рынки: США и ЕС
- Степень жесткости законодательства формирует фокус страхового продукта
- Страхование ответственности за потери персональных данных – основная доминанта
- Естественный спрос (перерыв в производстве и т.д.) – маргинален
- Киберстрахование не стало массовым видом

Российский рынок

Огромный потенциальный спрос – уровень цифровизации России на порядок выше «старого мира»

- Киберугрозы являются актуальными для российских предприятий
- Страхование не стало массовым по своим причинам:
- Малое количество страховщиков, способных предоставить капитал под новый тип рисков
- Высокая стоимость кибераудита
- Затруднения в сборе полноценной статистики об инцидентах

Статистика РФ подтверждает актуальность

96
компаний

Ежедневно становятся жертвами киберинцидентов и киберпреступлений

156
млрд ₽

Общий ущерб от киберпреступлений за 2023 год

20
млн ₽

Средний ущерб от кибератак у крупных российских компаний

168
утечек ПДн

Обнаружил Роскомнадзор по итогам 2023 года

03

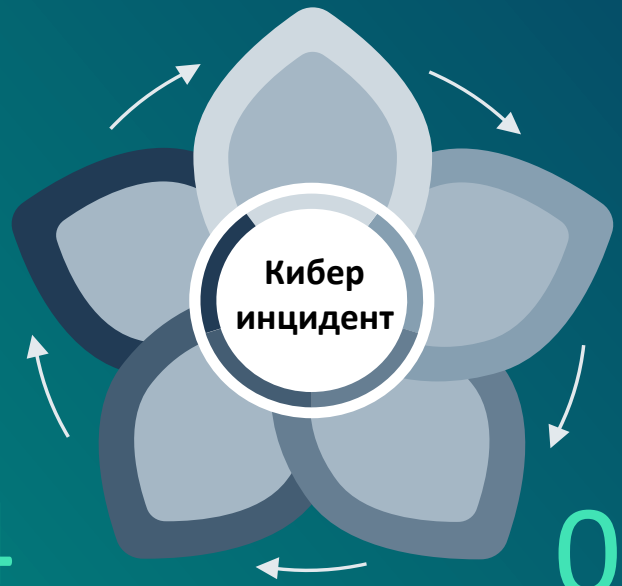
Продукты киберстрахования

Классическая пятерка страховых покрытий

01

Страхование информационных систем и информационных ресурсов:

- Программное обеспечение
- Корпоративная электронная почта
- Базы данных
- Web-сайт
- Облачный сервис (при условии, что он является собственностью страхователя)



02

Страхование от возникновения непредвиденных расходов:

- Расходы на расследование Инцидента
- Расходы на диагностику в связи с Инцидентом

03

Страхование убытков, возникших в результате перерыва в хозяйственной деятельности:

- Плата за аренду помещений
- Налоговые платежи
- Платежи в счет погашения основного долга и процентов по кредитам
- Заработная плата работникам Страхователя

04

Страхование гражданской ответственности:

- Имущество
- Жизнь, здоровье

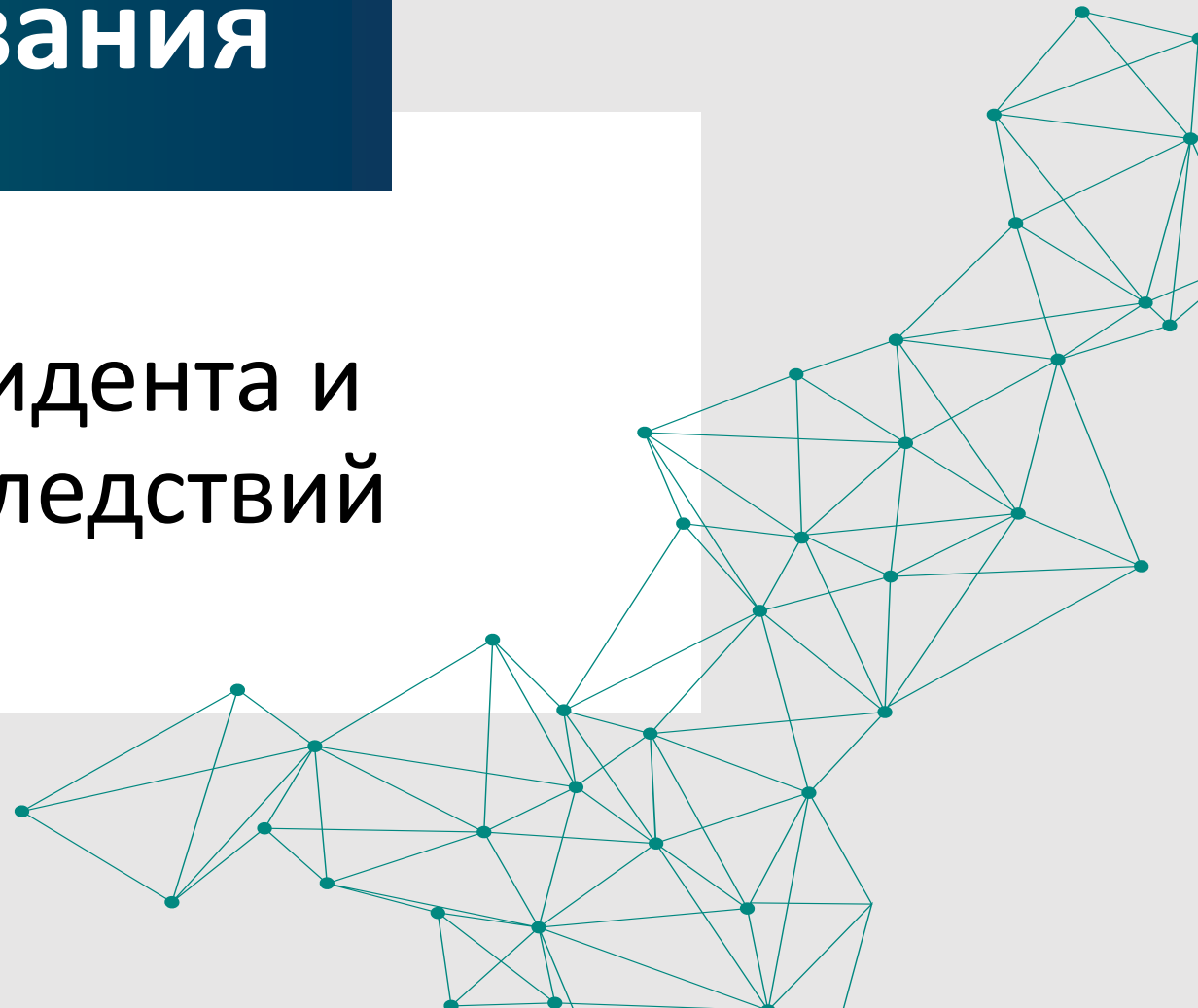
05

Страхование от несанкционированного списания денежных средств:

- со счетов страхователя
- корпоративных карт страхователя

Продукт киберстрахования

– это связка инцидента и финансовых последствий



Из чего складывается продукт киберстрахования:

01 Причины инцидентов + 02 Последствия инцидентов + 03 Андеррайтинг

- Шифрование данных, блокировка или создание помех в работе информационной системе или браузеров программой-вымогателем
- Нарушение работоспособности информационной системы, вызванное вредоносным программным обеспечением
- DoS/DDoS-атаки
- APT-атаки (целевые атаки)
- Атаки на уязвимости (нулевого дня) в системном ПО;
- Подключение компьютера к ботнету вследствие заражения системы вирусом через уязвимость ПО, невнимательнось пользователя (маскировка под «полезное содержимое»), использование санкционированного доступа к компьютеру
- Kill Chain («убийственная цепочка») и т.д.

- Ущерб информационным системам
- Перерыв в хозяйственной деятельности
- Нанесение вреда жизни, здоровью и имуществу третьих лиц
- Непредвиденные расходы
- Несанкционированное списание денежных средств со счета

- Простой
- Средний
- Сложный

В зависимости от величины страховой суммы

Программа страхования

04

Как организуются страховые операции по киберстрахованию

1 этап

Тарификация

Построение модели тарификации

01 Оценка частоты

- Оценка частоты инцидентов кибербезопасности
- Оценка конвертации инцидента в предусмотренные договором страховые случаи, как условная вероятность:
  - физические риски
  - вред информационным системам/базам данных
  - утечка данных
  - ГО за причиненный вред и ущерб третьим лицам
  - Доп. расходы в связи с инцидентом (юридические, PR, расследование и т.д.)
  - другие покрытия.

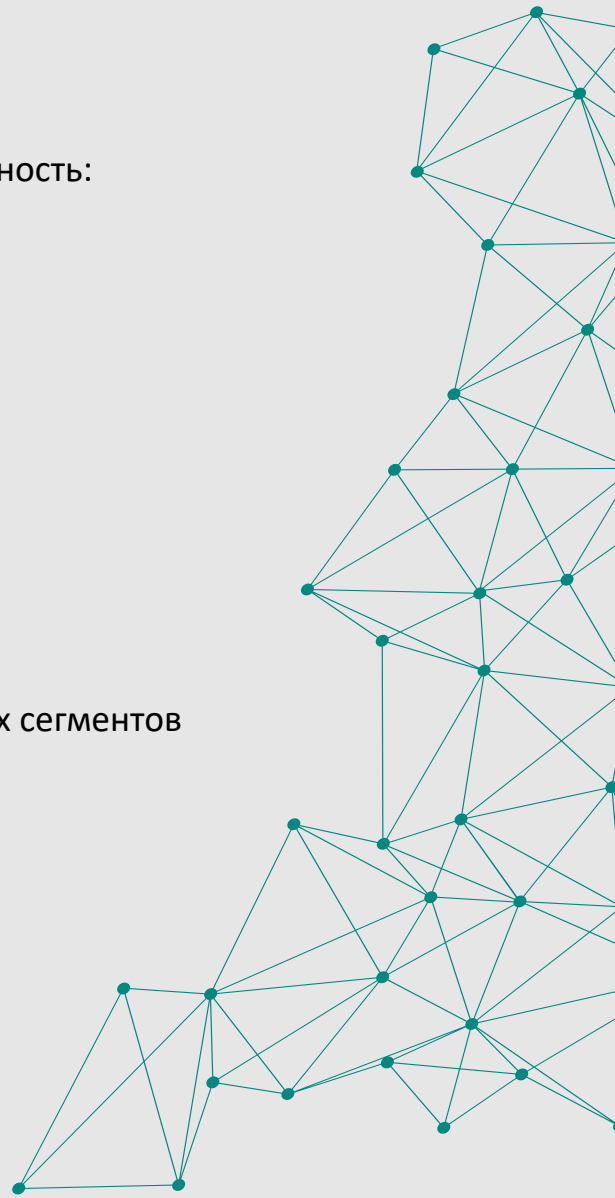
02 Оценка средней тяжести

- Определение диапазонов страховых сумм (сегментация портфеля)
- Оценка ущерба для максимальной страховой суммы, не требующей установления лимитов
- Интерполяция величины ущерба для меньших страховых сумм – оценка утилизации СС для различных сегментов
- Оценка расходов на урегулирование

03 Расчет нетто-ставок

04 Определение показателей нагрузки в структуре ставки: комиссия, прочая аквизиция, операционные расходы

05 Расчет брутто-ставок



2 этап

Процесс андеррайтинга

Основные факторы, способные повлиять на оценку страхового риска при страховании информационных рисков (киберрисков)

1) вид деятельности Страхователя, отрасль;

2) размер организации, организационная структура

3) география бизнеса организации

4) используемые Страхователем Компьютерные системы

5) количество и тип хранимых персональных данных

6) наличие онлайн активности и онлайн-продаж

7) возможный размер ущерба от Перерыва в производстве

8) уровень информационной защиты Страхователя, в том числе наличие и вид программ антивирусной защиты, обучение персонала, политика подключения внешних устройств и т.д.

9) политика и процедуры внутреннего контроля (в том числе сетевая безопасность, процедуры резервного копирования и т.д.)

10) наличие и особенности плана реагирования на Киберинцидент или Перерыв в производстве

11) привлечение Страхователем контрагентов, использование Страхователем облачных сервисов

12) наличие в прошлом убытков и инцидентов, связанных с информационными рисками, предлагаемым к страхованию

13) соблюдение требований Регулятора

Способы заключения договора страхования в России

«Пакет»

- Заключение договора страхования «автоматическое» - без аудита кибер защищенности
- Страховая защита стандартная и цена фиксированная,
- Страхование кибер рисков является частью более широкого страхового договора (страхования имущества и т.п.)
- Небольшие страховые суммы (например до 1-5 млн рублей)
- Страховая выплата компенсирует ограниченный перечень потерь – например, только перерыв в производстве

«Конструктор»

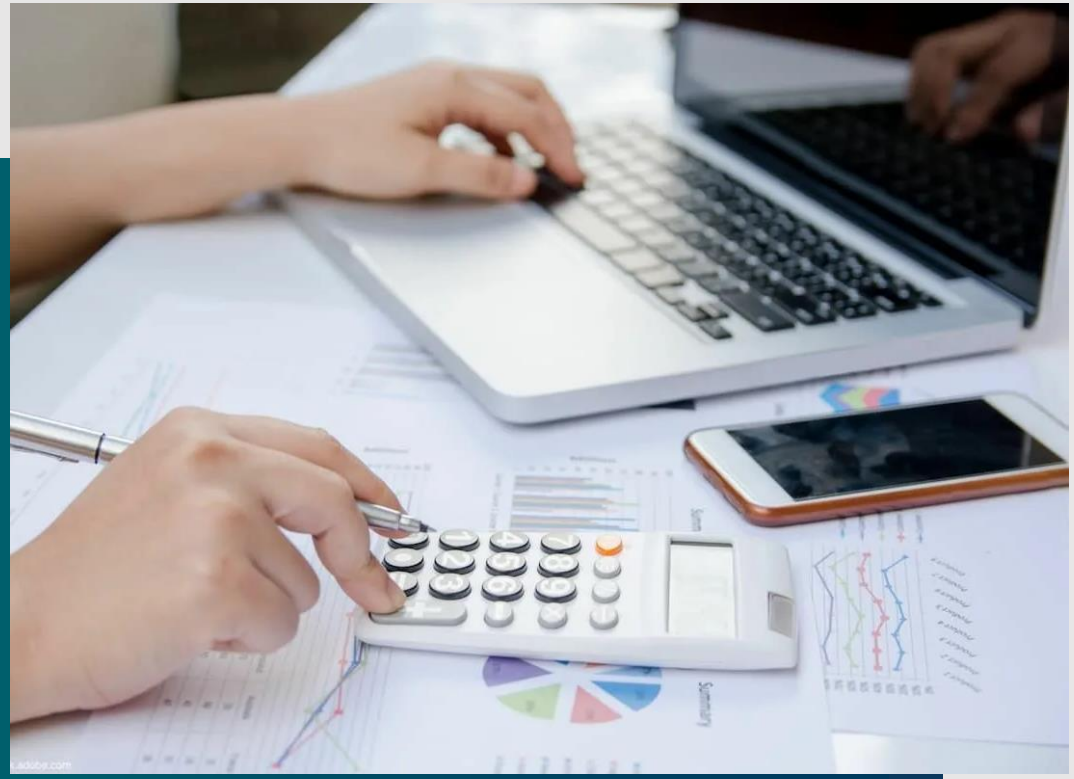
- Упрощенный аудита уровня киберзащищенности Клиента
- Анкетирование и скоринг
- Заключение (или отказ) договора страхования на основании скоринга
- Возможность выбрать страховую защиту из нескольких вариантов, фиксированное ценообрахование
- Страховые суммы от 3-5 до 20-25 млн рублей, срок подготовки договора – до 1 недели

«Полный цикл»

- Проведение аудита уровня киберзащищенности Клиента
- Анкетирование
- Проведение интервью с ключевыми сотрудниками
- Тестирование информационных систем на уязвимость
- Заключение (или отказ) договора страхования на основании результатов аудита
- Возможность подстроить страховую защиту под профиль предприятия, гибкое ценообразование
- Страховые суммы от 25 млн рублей и выше, срок подготовки договора – от 2 месяцев

3 этап

Процесс урегулирования убытков



При возникновении событий, имеющих признаки страхового случая, к процессу урегулирования убытков могут привлекаться эксперты в области информационных технологий, которые обеспечивают:

01 оперативное реагирование, обнаружение и расследование причин Киберинцидента

02 диагностику Компьютерной системы

03 устранение проблем

04 минимизацию потерь от Киберинцидента

05 мониторинг проблемных сегментов

06 определение размера ущерба в результате Кибератаки

Если данные опции включены в программу страхования

! Такие необходимые, разумные и целесообразные расходы на привлечение экспертов в области информационных технологий **могут подлежать возмещению** по договору страхования, если они были предварительно одобрены Страховщиком и наступившее событие признано страховым случаем

4 этап

Взаимодействие с партнерами

Модель взаимодействия (пример)

Функции:

- Предстраховой аудит клиента и рекомендации по улучшению безопасности (крупные объекты)
- Содействие в создании скоринг модели для страхования (массовые объекты)
- Экспертиза и фиксация страхового случая
- Проведение расследования инцидентов
- Консультирование

Функции:

- Определение страхового покрытия и тарифов
- Разработка страховых продуктов
- Страхование – компенсация потерь клиентам
- Оплата услуг по фиксации страхового случая (за счет расходов на ведение дела)
- Финансирование за счет страховых выплат услуг по расследованиям и восстановлению после кибер инцидентов

Функции:

- Предоставление потенциальной клиентской базы (на основе профиля целевого сегмента)
- Продажи через каналы

05

Проблемы индустрии киберстрахования

Проблемы индустрии киберстрахования

01 Страховая индустрия не спешит предлагать широкое покрытие по киберстрахованию

02 Нечеткая и «разношерстная» законодательная база по странам мира

03 Дефицит компетенций в области киберзащиты и безопасности, по оценке рисков

04 Нет достаточной инфраструктуры по фиксации и урегулированию страховых случаев

05 Потенциальная потребность клиентов в страховании и киберзащите не превратилась в сформированный спрос

06 Высокие риски убыточности, особенно на начальном этапе становления рынка:

- существенные сложности с получение полной и достоверной статистике
- жертвы киберинцидентов склонны не афишировать свои проблемы
- частота киберинцидентов имеет тенденцию к росту

06 Достижения Сбербанк Страхования

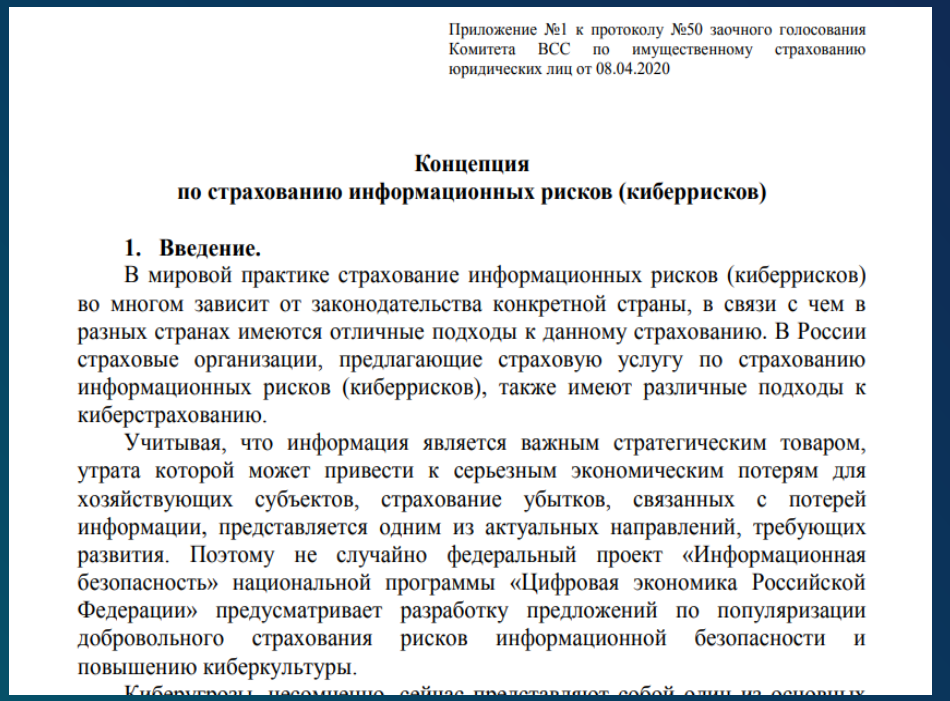
- 6 лет на рынке киберстрахования
- 4 поколения продуктов
- Доступность через цифровые и оффлайн каналы
- Более 4 тыс. клиентов ЮЛ
- Реальный опыт урегулирования убытков

07

Рабочая группа BCC по страхованию информационных рисков (киберрисков)

РЕЗУЛЬТАТЫ НА УРОВНЕ ВСС:

- Концепция страхования киберрисков (2021 г.)
- Методические рекомендации по оценке рисков (2022 г.)
- Регулярные мероприятия по популяризации киберстрахования
  – Выступления в секциях ТПП
  – Семинары для страховщиков
  Ближайший семинар – 26 сентября 2024 !
  – Конференции
- Взаимодействие с Советом Федерации по внедрению страхования ответственности за утечки персональных данных



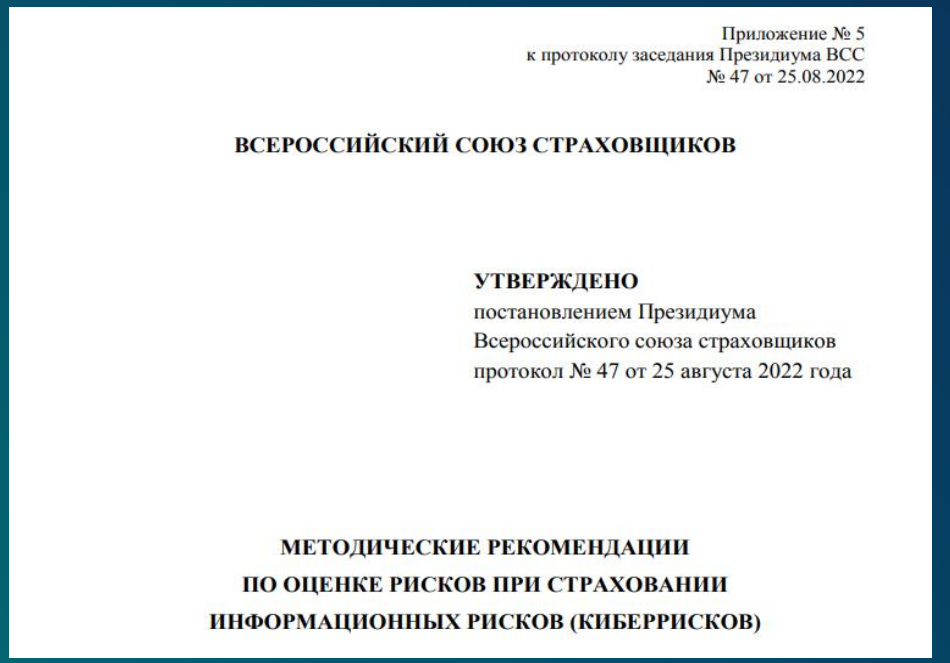
Приложение №1 к протоколу №50 заочного голосования Комитета ВСС по имущественному страхованию юридических лиц от 08.04.2020

Концепция
по страхованию информационных рисков (киберрисков)

1. Введение.

В мировой практике страхование информационных рисков (киберрисков) во многом зависит от законодательства конкретной страны, в связи с чем в разных странах имеются отличные подходы к данному страхованию. В России страховые организации, предлагающие страховую услугу по страхованию информационных рисков (киберрисков), также имеют различные подходы к киберстрахованию.

Учитывая, что информация является важным стратегическим товаром, утрата которой может привести к серьезным экономическим потерям для хозяйствующих субъектов, страхование убытков, связанных с потерей информации, представляется одним из актуальных направлений, требующих развития. Поэтому не случайно федеральный проект «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» предусматривает разработку предложений по популяризации добровольного страхования рисков информационной безопасности и повышению киберкультуры.



Приложение № 5
к протоколу заседания Президиума ВСС
№ 47 от 25.08.2022

ВСЕРОССИЙСКИЙ СОЮЗ СТРАХОВЩИКОВ

УТВЕРЖДЕНО
постановлением Президиума
Всероссийского союза страховщиков
протокол № 47 от 25 августа 2022 года

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
ПО ОЦЕНКЕ РИСКОВ ПРИ СТРАХОВАНИИ
ИНФОРМАЦИОННЫХ РИСКОВ (КИБЕРРИСКОВ)

Мы хотим, чтобы:

1. Операторы персональных данных несли финансовую ответственность
2. Каждый гражданин был защищен и получал финансовую компенсацию за потерю персональных данных
3. Владелец персональных данных имел возможность выбрать защиту из:
   - Банковской гарантии
   - Собственных средств
   - Страхования

Сложности:

1. Оценить стоимость персональных данных
2. Обеспечить объективный механизм фиксации фактов утечки и последствий для физ. лица
3. Создать удобный и современный механизм урегулирования убытков, получения страховой выплаты и защиты от мошенников с обоих сторон

Ответы на вызовы:

Будут реализованы в типовом страховом продукте ВСС