РОССИЙСКАЯ
НАЦИОНАЛЬНАЯ
ПЕРЕСТРАХОВОЧНАЯ
КОМПАНИЯ

Кибер-страхование. Начало большого пути

Ноябрьские деловые встречи

МОСКВА | НОЯБРЬ 2017

Кибер-страхование. Предпосылки возникновения

Развитие технологий

(Big Data, искусственный интеллект, block chain, интернет вещей, облачные решения, соцсети, автоматизация промышленных производств, критической инфраструктуры, развитие онлайн-сервисов, e-commerce, рост объемов электронных транзакций

- Участившиеся целенаправленные хакерские атаки на бизнес
- Угроза кибер-терроризма
- Рост уязвимости и убытков

Инциденты в мире. Зарубежный опыт.

- 2003. США. Вирусный червь Slammer обрушил корпоративную сеть атомной электростанции в штате Огайо, после чего распространился на системы мониторинга безопасности и охлаждения станции. Главный компьютер электростанции после этого вышел из строя. На восстановление систем ушло шесть часов.

- 2010. Иран. Около 30 тыс. компьютерных систем промышленных объектов были заражены вирусом Stuxnet. Взлом привел к остановке работы более 1,3 тыс. центрифуг по обогащению урана в Натанзе и переносу сроков запуска АЭС "Бушер".

- 2013. США. Перехват иранскими хакерами контроля над плотиной возле Нью-Йорка

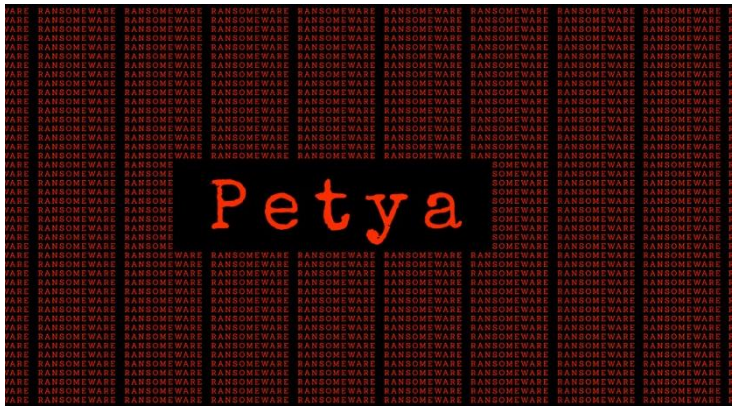
- 2013. Взлом персональных данных 2 млн клиентов Vodafone

- 2014. Южная Корея года в Южной Корее хакеры получили доступ к внутренней сети оператора Hydro and Nuclear Power Co Ltd. Проникнуть в сеть удалось после рассылки сотрудникам компании более 5,9 тыс. зараженных писем. В дальнейшем злоумышленники требовали остановки реакторов на АЭС "Кори" и "Вольсон", а также публиковали схемы, внутренние инструкции и данные о сотрудниках.

- 2016. германия. Компьютеры АЭС "Гундреммингенн" (120 км от Мюнхена) энергетической компании RWE оказались заражены вирусами W32.Ramnit и Conficker. Вредоносное ПО обнаружили на 18 съемных носителях информации в компьютерной системе блока Б — в программном обеспечении визуализации данных.

Инциденты в России.

Май 2017



Под ударом хакеров, оказались железные дороги, больницы, правительственные учреждения. Также о попытках взлома говорили в Центробанке, МВД, МЧС, компаниях связи.

Взломанные злоумышленниками сети промышленных предприятий:

- МОТОВИЛИХА – ПАО «Мотовилихинские заводы»
- НПО им. С.А. Лавочника
- НПП Рубин

Кибер-страхование. Источники спроса

- Операторы связи
- Финансовые организации
- E-commerce
- Фарма, медицина
- ТЭК
- Промышленность
- Транспорт

- Развитие технологий (Big Data, искусственный интеллект, автоматизация производств, критической инфраструктуры)
- Развитие онлайн сервисов, e-commerce
- Участившиеся целенаправленные хакерские атаки на бизнес
- Угроза кибер – терроризма
- Рост уязвимости бизнеса
- Риск наступления ответственности за утечку персональных данных
- Увеличение спроса со стороны страхователей

Страхование от кибер - рисков

США* – 90% мирового рынка кибер-страхования

Обязанность бизнеса декларировать утечку персональных данных

Судебные прецеденты по массовым искам за разглашение персональных данных (ответственность перед третьими лицами)

Законодательно допустимо страхование выкупа

2016 год в США производители заплатили за кибер-страхование $36,9 млн (рост 89%)

Европа*

Рост мирового рынка кибер-страхования от 25% - 50%

Объем рынка $2,5 млрд.в 2014 году , рост до $7,5 млрд. в 2020

2019 году убытки от киберпреступлений составят $2 трлн.

64.000 актов киберпреступности было официально зарегистрировано в Германии в 2012 году (42 млн евро ущерба)

Россия

У нескольких компаний есть базовые продукты

Процедуры принятия рисков на страхование достаточно сложны

*Источники: PwC, WSJ, Allianz, Берлин.24

Кибер-страхование. Покрытие

Ответственность перед третьими лицами

Расходы на восстановление данных и инфраструктуры

Убытки от перерыва в деятельности

Имущественный ущерб

Страхование выкупа (запрещено в России)

Кибер-страхование. Перспективы развития в России

Введение к 2020 году индустриального стандарта по обязательному аудиту информационной безопасности

Создана Рабочая группа по кибер-страхованию в рамках проекта «Цифровая экономика»

Обсуждение возможности введения вмененного кибер-страхования для объектов критической инфраструктуры.

Кибер-страхование. Роль РНПК

Продвижение кибер-страхование в России

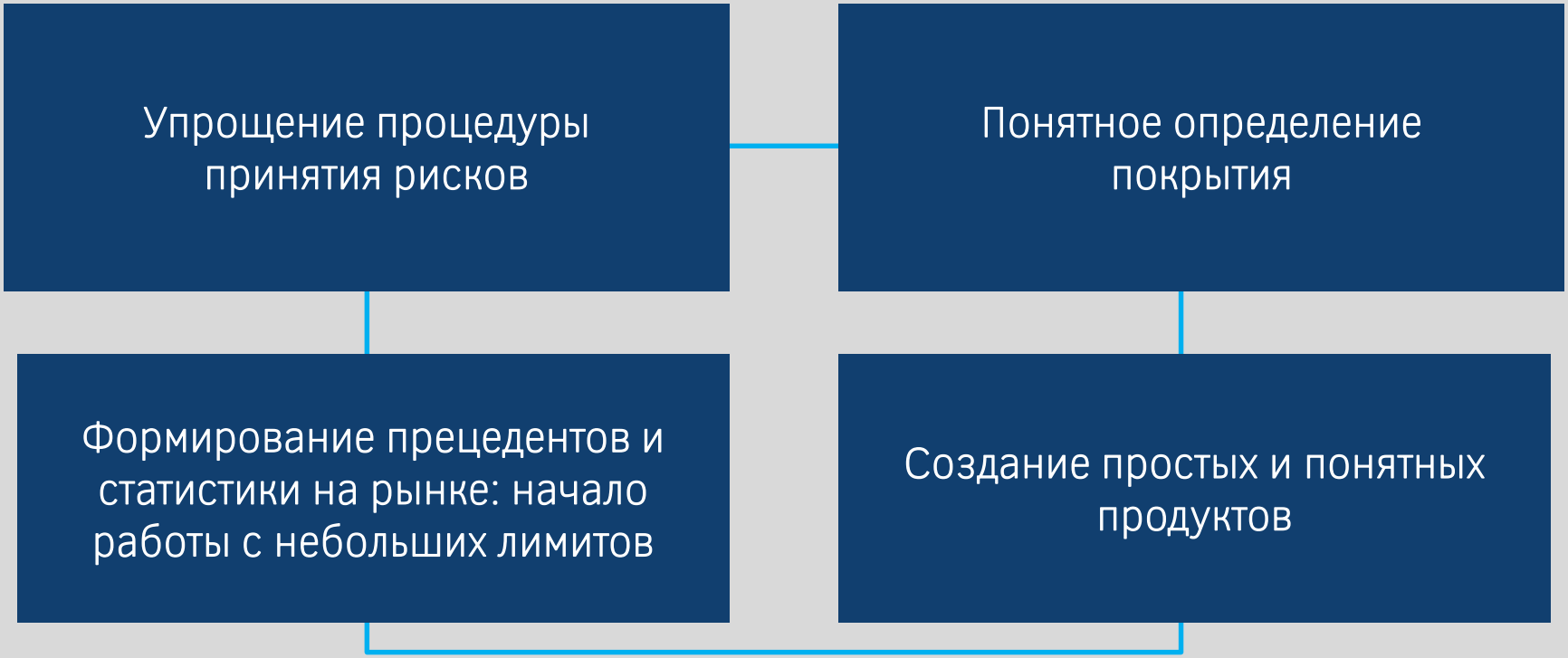
Создание новых продуктов

Предоставление емкости

Кибер-страхование. Барьеры развития

- Низкое проникновение, недостаток кейсов
- Специфика российского законодательства
- Судебная практика еще не сложилась, отсутствие прецедентов
- Недоверие к институту страхования и недостаточная страховая грамотность
- Отсутствие компетенций и опыта у российских страховых компаний
- Технические сложности организации (пере) страхования, урегулирования убытков

Кибер-страхование. Что нужно потребителю?



РОССИЙСКАЯ
НАЦИОНАЛЬНАЯ
ПЕРЕСТРАХОВОЧНАЯ
КОМПАНИЯ

СПАСИБО ЗА ВНИМАНИЕ!

Москва, 125047 | Гашека, 6 | БЦ «Дукат Плейс III»
Тел +7 (495) 730 44 80 | факс +7 (495) 730 44 79 | rnrc@rnrc.ru

www.rnrc.ru