

# КИБЕР-РИСКИ: предстраховая экспертиза, страхование и урегулирование убытков



**labb**

Loss Adjusters Bureau

| GROUP | iB |

GLOBAL CYBER SECURITY COMPANY

# Введение

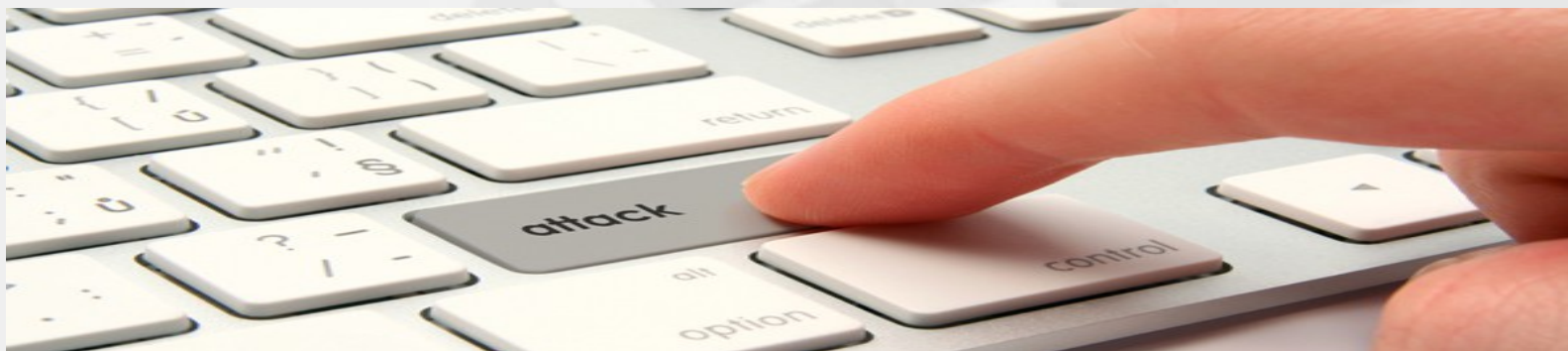


- Мировая экономическая система находится на постиндустриальной (информационной) стадии развития
- Глобальная информационная сеть Интернет – охватывает практически весь земной шар
- «Умные» устройства и новые услуги могут быть причиной непредвиденных последствий и уязвимостей
- Возникли специфические риски – кибер-риски
- В рамках отчета по глобальным рискам 2015 г. Международного экономического форума (World Economic Forum), виртуальные (кибер-) риски названы одними из ключевых коммерческих рисков.
- Новый вид страхования – страхование кибер-рисков

# Кибер-риски: определение



- **Кибер-риск** - Риск, связанный с использованием компьютерного оборудования и программного обеспечения, как в местных (локальных) сетях, так и в глобальной Интернет-сети; в расчетно-платежных системах, системах интернет-торговли, промышленных системах управления; а также риск, связанный с накоплением, хранением и использованием личных персональных данных.



# Кибер-риски: текущее положение



- Сотни тысяч событий и десятки тысяч зарегистрированных преступлений в мире.
- Количество официально зарегистрированных преступлений в Украине в области IT: в 2014 году – 4 800, 2015 году – 6 025. Рост более чем на 25,00%
- Совокупный размер ущерба мировой экономике в 2014 по оценке американской корпорации Intel составил около 400 млрд. долл. США.
- В зоне основного риска – организации финансового сектора, ТЭК, промышленности, здравоохранения.

# Кибер-риски: прогнозы



- Рост общего количества событий
- Увеличение количества целевых атак
- Умеренный рост банковского фишинга
- Рост инцидентов с банкоматами
- Распространение за пределы финансового рынка
- Осознание необходимости страхования подобных рисков, рост объемов страхования



# Кибер-риски: виды событий



1. Нецелевые атаки (фишинг, кардинг, sms мошенничество)
2. Целевые атаки (финансовое мошенничество, хищение баз данных, промышленный шпионаж, DDoS атаки, вымогательство)
3. Атаки изнутри (хищение, уничтожение информации, содействие целевой атаке)



**VIRUS**



# Кибер-риски: возможные убытки



- 1. Прямой ущерб (хищение средств, утрата информации, повреждение ПО, поломка оборудования и т. п.)
- 1. Убытки от перерыва в коммерческой деятельности
- 1. Ответственность перед третьими лицами (за нанесенный вред, разглашение информации)
- 1. Ущерб вследствие промышленного шпионажа и хищения интеллектуальной собственности
- 1. Ущерб репутации компании
- 1. Дополнительные расходы (антикризисный-PR, юридические услуги и т. д.)

# Кибер-риски: особенности



1. Специфичность рисков и убытков
1. Отсутствие у страхователей и страховщиков планов по реагированию в подобных случаях
1. Большинство событий вызваны умышленными действиями – перспектива суброгации
1. Целесообразность привлечения профессиональных консультантов на этапе заключения полиса и урегулирования убытка



# Примеры



- Хакеры из Украины стали участниками международной киберпреступной группировки Carbanak, которая за два года похитила примерно \$1 млрд из более чем 100 финансовых учреждений по всему миру. Помимо украинцев, в «ограблении века» принимали участие хакеры из России, Китая и ряда других стран. Расследование началось с инцидента, когда в конце 2013 года один из киевских банкоматов начал бессистемно «выплевывать» деньги под ноги прохожих. Оказалось, что это была наименьшая из проблем банка, которые впоследствии удалось вскрыть в ходе расследования
- Служба безопасности Украины установила личность и задержала 38-летнего киевлянина, занимавшегося хищением средств со счетов клиентов иностранных и отечественных финансовых учреждений и причастного к вмешательству в работу компьютерных систем одного из иностранных банков, в результате чего в 2008 году было похищено свыше \$9 млн.
- В 2015 году на территории Украины Европол при участии правоохранителей из шести европейских стран были задержаны пять человек, которых обвиняют в создании крупной хакерской группировки. Задержанных подозревают в разработке и эксплуатации известных банковских троянов Zeus и SpyEye, которые они распространяли на территории Европы и за ее пределами, в результате чего были украдены значительные суммы со счетов крупнейших мировых банков. Предварительная оценка ущерба - не менее 2 млн евро.

# Страхование кибер-рисков: виды страхования



- Покрытие в рамках имущественного страхования: поломка оборудования; перерывы в производстве; страхование интеллектуальной собственности.
- Покрытие в рамках страхования ответственности: общегражданская ответственность; страхование профессиональной ответственности; страхование ответственности товаропроизводителя;
- Fidelity
- BVV
- Покрытие в рамках страхования кибер-рисков/ кибер-ответственности (покрывает собственный ущерб и ущерб причиненный третьим лицам)

# Страхование кибер-рисков в рамках традиционных полисов: пробелы покрытия



- По полису имущественного страхования: возмещается только имущественный ущерб; ответственность не покрывается; как правило, кибер-риски вообще исключаются из покрытия
- При страховании ответственности: возмещается ущерб причиненный третьим лицам; собственный ущерб страхователя не покрывается.
- Fidelity – покрывает ущерб от умышленных действий собственных сотрудников
- BBV – учитывает специфику и доступен только финансовым учреждениям

# Поккрытие по кибер- рискам:



- Покрывается собственный ущерб и вред, причиненный третьим лицам
- Собственный ущерб: поломка оборудования; перерывы в производстве; потеря информации; суммы вымогательств; расходы на урегулирование; штрафные санкции.
- Ущерб третьих лиц: материальный ущерб; моральный вред; нарушение прав интеллектуальной собственности



**LABB – международная компания, специализирующаяся в области независимого расследования и урегулирования убытков. Возможность оказания сюрвеерских и аджастинговых услуг в более чем 140 странах мира.**

- **Расследование и урегулирование крупных и технически сложных событий**
- **Расчет различных видов убытка (в том числе, от перерыва в производстве)**
- **Предстраховая экспертиза**

**Group IB – одна из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничества с использованием высоких технологий.**

- **Предотвращение и мониторинг (в том числе аудит информационной безопасности)**
- **Компьютерная криминалистика и расследование инцидентов**
- **Разработка и внедрение специализированного ПО**



# **Предлагаемые продукты**

- 1. Предстраховая экспертиза объектов в части кибер-рисков при заключении договора страхования (pre-risk)**
- 1. Расследование и урегулирование убытков в период действия полиса**



# **Pre-risk (полный)**

- **Оценка рискозащищенности объекта**
- **Определение возможных угроз**
- **Разработка сценариев наиболее вероятных убытков**
- **Рекомендации по повышению уровня защищенности и предотвращению возможных убытков**
- **Разработка инструкций по действиям в случае чрезвычайных ситуаций**
- **Определение возможного влияния кибер-рисков на производственную деятельность**
- **Расчет финансовых показателей и возможных убытков**
- **Подготовка отчета**





# Pre-risk (упрощенные модели)

- **Стресс-тест (от 3 рабочих дней)**
  - Сетевая разведка аффилированных сетевых ресурсов
  - Автоматизированное сканирование уязвимостей
  - Ручная эксплуатация выявленных уязвимостей
  - Нагрузочное тестирование критичных ресурсов
  - Подготовка краткого отчёта о степени защищенности информационных активов компании, доступных извне
- **Экспресс-тест (1 полный рабочий день)**
  - Автоматизированное сканирование уязвимостей
  - Подготовка справки о защищенности компании

# Урегулирование убытков



- Срочное реагирование на возникающие угрозы (пресечение действий, рекомендации по минимизации ущерба)
- Расследование обстоятельств и причин убытка, поиск виновника
- Юридический анализ, определение факта наступления страхового случая
- Привлечение авторитетных юристов в случае необходимости. Наш постоянный партнер – компания C'M'S'
- Расчет размера понесенных убытков
- Оценка перспектив суброгации и содействие в реализации требования
- Подготовка отчета с рекомендацией по урегулированию и согласование результатов со страховым рынком



- Развитие информационных технологий неизбежно влечет за собой увеличение кибер-рисков
- Одним из способов управления этими рисками является страхование
- Страхование кибер-рисков одно из наиболее перспективных направлений развития страхового бизнеса.
- Задача страхового сообщества аргументировано подсказать владельцам кибер-рисков решение вопроса минимизации убытков путем передачи данных рисков в страхование.
- Разрабатываемые, в ходе создания страховой программы меры защиты в значительной степени предохраняют от таких рисков.

# Заключение:



- Развитие информационных технологий неизбежно влечет за собой увеличение кибер-рисков
- Одним из способов управления этими рисками является страхование
- Страхование кибер-рисков одно из наиболее перспективных направлений развития страхового бизнеса.
- Задача страхового сообщества аргументировано подсказать владельцам кибер-рисков решение вопроса минимизации убытков путем передачи данных рисков в страхование.
- Разрабатываемые, в ходе создания страховой программы меры защиты в значительной степени предохраняют от таких рисков.

# Контакты



**Сергей Онищенко**

**Директор**

**моб.: +38 095 790 17 36**

**e-mail: [sonyshchenko@lossadjuster.com.ua](mailto:sonyshchenko@lossadjuster.com.ua)**

**Олег Кирбаба**

**Директор по развитию**

**моб.: +38 099 174 47 84**

**e-mail: [okirbaba@lossadjuster.com.ua](mailto:okirbaba@lossadjuster.com.ua)**

**Спасибо за внимание!**

