



- **580 млрд. рублей** – прямые потери российских компаний в 2017 году*
- **\$1 триллион** – общемировые потери в результате кибер-атак**
- **80%** компаний не подозревают или скрывают факт успешной кибер-атаки*
- **46%** малых предприятий и **62%** крупных предприятий в 2017 были атакованы
- **5,3 млн. руб.** средний убыток в российской компании до 1000 человек***
- **16,4 млн. руб.** средний убыток в российской компании до 5000 человек***
- **3 млрд. руб.** к 2025 году составят страховые премии на российском рынке.

* По подсчетам Аналитического центра Национального агентства финансовых исследований (НАФИ)

** По данным всемирного экономического форума

*** Представленные данные основаны на результатах онлайн-опроса проведенного в 2018 году "Лабораторией Касперского" и исследовательской компанией B2B International.

Кибератака на МВД остановила выдачу водительских прав и техосмотр

В мае 2017 года работа системы выдачи водительских прав в нескольких регионах России парализована из-за вирусной атаки на компьютеры МВД, проблемы возникли не только при выдаче прав, но и при проведении любых действий с автомобилями, требующих компьютерной регистрации. Так, многие водители по этой причине не могли пройти техосмотр.

За одну неделю в декабре 2014 года Сбербанк потерял 1,3 трлн. рублей

В результате информационной атаки в декабре 2014 года Сбербанк потерял 1,3 трлн рублей наличных денег, или 300 тонн наличности, за одну неделю. В период «черного вторника» клиентам Сбербанка было разослано более миллиона sms-сообщений о проблемах в банке. За этим последовала вторая волна sms, которая и привела к панике и очередям у банкоматов.

На «Роснефть» совершена мощная кибератака

Серверы нефтяной компании «Роснефть» подверглись мощной хакерской атаке, сообщается в Twitter госкомпании. Все компьютеры в «Башнефти», которая принадлежит «Роснефти», перезагрузились, скачали неустановленную программу, вывели на экран заставку вируса WannaCry и предложили заплатить 300 долларов в биткоинах за разблокировку.

В результате разрушения доменной печи сталелитейный завод в Германии потерял 100 млн. евро.

Атакующие использовали рассылку писем с вредоносным ПО под видом корпоративных рассылок и «сложные техники социальной инженерии», чтобы получить доступ к офисной сети предприятия, откуда смогли попасть в промышленную сеть. После заражения промышленного сегмента, говорят следователи, начались «контролируемые» сбои на одной из доменных печей завода, в результате чего печь перегрелась и расплавилась.

«Инвитро» заявила об ущербе от кибератаки

Медицинская компания «Инвитро» приостановила сбор биоматериала и выдачу результатов анализов пациентов из-за хакерской атаки 27 июня 2017 года. Ежедневно «Инвитро», по словам ее представителя, проводит в среднем 27 000 исследований. Материальный ущерб для «Инвитро» составил 1,5–2% годового оборота.

Maersk потеряла \$300 млн из-за шифровальщика NotPetya

Такая сума была отражена в качестве потерь в финансовом отчете компании за второй квартал 2017 года. От заражения пострадали компании Maersk Line (крупнейший в мире оператор контейнерных перевозок), оператор APM Terminals и логистическая компания Damco. Заражение произошло посредством установки новой версии программы электронного документооборота, в которую был встроен вирус киберпреступниками без ведома разработчика.

Что это?

Последний рубеж обороны от актуальных и перспективных вызовов современности, когда все прочие средства защиты оказались бессильны. Нет технической 100% защиты.

Кибер-страхование предлагают уже более 80 страховщиков во всем мире, существует на Западе более 5 лет, 30% компаний в США уже застрахованы.

Для кого?

Для всех, кто использует компьютерные системы в своей деятельности, а особенно для операторов персональных данных, провайдеров услуг, финансовых, промышленных, торговых и логистических компаний.

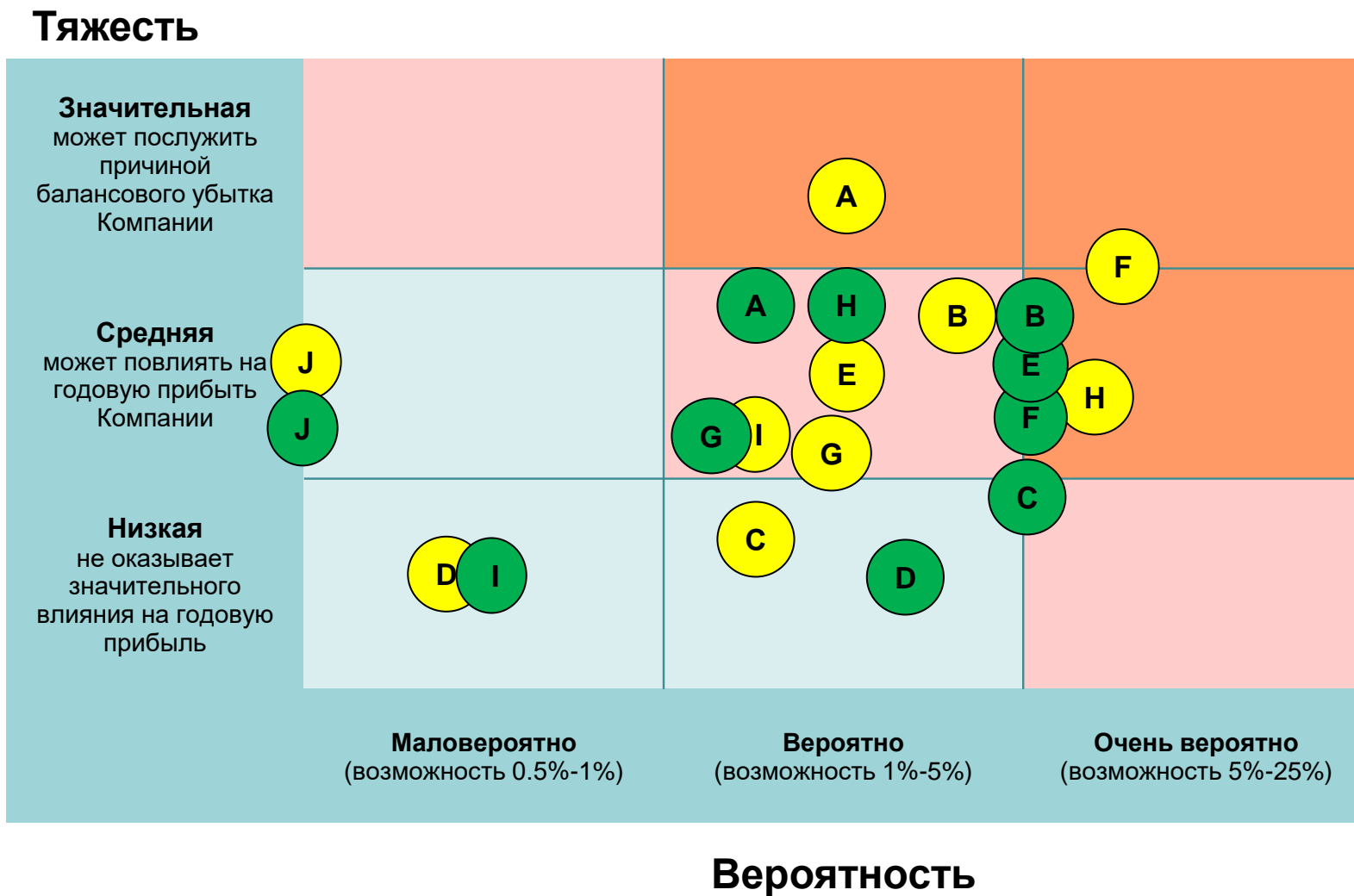
Большинство действующих программ страхования исключают электронные риски.

Почему сейчас?

- Проникновение компьютерных и сетевых технологий во все сферы;
- Экспоненциальный рост количества компьютерных атак в 2016-18 гг.;
- Увеличение размера среднего убытка от кибер-инцидента;
- Цифровая экономика;
- Индустрия 4.0;
- 187-ФЗ о КИИ.

● - предприятия среднего и малого бизнеса** ● - предприятия крупного бизнеса

A	Кража интеллектуальной собственности
B	Перерыв в деятельности
C	Утрата данных и программного обеспечения
D	Кибер-вымогательство
E	Кража денег
F	Нарушение конфиденциальности
G	Ответственность перед третьими лицами
H	Ущерб репутации
I	Гибель и повреждение имущества
J	Вред жизни и здоровью



*По материалам брокера Guy Carpenter, London

** Перерыв в деятельности, кража денег, нарушение конфиденциальности (в т.ч. персональных данных) и утрата ПО – наиболее вероятные риски для предприятий среднего и малого бизнеса



- При заключении договора кибер-страхования АльфаСтрахование проводит один из трех типов оценки:

Уровень	Страховая сумма	Способ оценки	Описание
1 уровень	до 25 млн. руб.	Анкета	
2 уровень	от 25 до 150 млн. руб.	Анкета + Эксперт	Визит включает интервью + частичный осмотр и длится в среднем 2-4 часа
3 уровень	более 150 млн. руб.	Анкета + Оценка партнёра	Оценка риска проводится партнёром

- Индивидуальный расчёт, коробки с партнёрами.
- Мы проводим оценку риска самостоятельно и с привлечением независимых экспертов, признанных лидер отрасли кибербезопасности.
- Если Страхователь уже проводит аудит IT-безопасности и/или имеет сертификат ISO 27001/2, то повторный аудит или выезд эксперта не требуется – для оценки риска могут быть использованы результаты уже проведенного Страхователем аудита.

Страховая сумма	Примерные тарифы
до 5 млн. руб.	1-2%
5-25 млн. руб.	0.75-1.75%
25-150 млн. руб.	0.5-1.5%
более 150 млн. руб.	0.25-1.25%



Наши приоритеты:

Решение проблемы

в первую очередь мы стремимся устранить причину проблемы чтобы свести к минимуму негативные последствия

Быстрое урегулирование

затем мы стремимся в кратчайшие сроки урегулировать инцидент и выплатить страховое возмещение

Пример:

Этап	Диагностика и экспертиза	Восстановление системы и данных	Публичные заявления	Правовая поддержка	Оценка убытка
1 - Устранение	Идентификация проблемы и привлечение ресурсов, требуемых для решения	Предупреждение любой дальнейшей атаки или заражения	Начало публичных заявлений	Назначение юристов для обеспечения конфиденциальности и	Оценка потенциального убытка
2 - Управление	Экспертиза для установления степени повреждения	Восстановление системы и потерянных данных	Продолжение публичных заявлений, Уведомления вовлеченных третьих лиц	Коммуникации с вовлеченными третьими лицами	Расследование убытка по перерыву в производстве
3 - Урегулирование		Проверка безопасности и составление плана для предотвращения в будущем		Урегулирование претензий третьих лиц	Расчет и урегулирование убытка по ВІ



ВСЕ УГРОЗЫ ЛИКВИДИРОВАНЫ



GLOBAL BANKING &
Finance
review®

«АльфаСтрахование» три года, в 2013, 2014 и 2017 г.г., становилась победителем международной премии **Global Banking & Finance Review** в номинации **«Лучшая российская страховая компания»** (Best Insurance Provider Russia)