БИЗНЕС БЕЗ ОПАСНОСТИ

Как оценить ущерб от киберрисков?

Алексей Лукацкий

Бизнес-консультант по безопасности

alexey@lukatsky.ru

Универсальные вопросы для начала разговора о рисках

- Что остановит или замедлит операции в вашей организации?
- Что приведет к снижению прибыли / выручки / маржинальности / доли рынка вашей компании?
- Что приведет к снижению качества предоставляемого продукта / услуги?
- Что приведет к негативному влиянию на цель компании / бизнес-подразделения / бизнес-проекта / executive sponsor?

Как обычно измеряют риски/угрозы ИБ?

Двухфакторная оценка

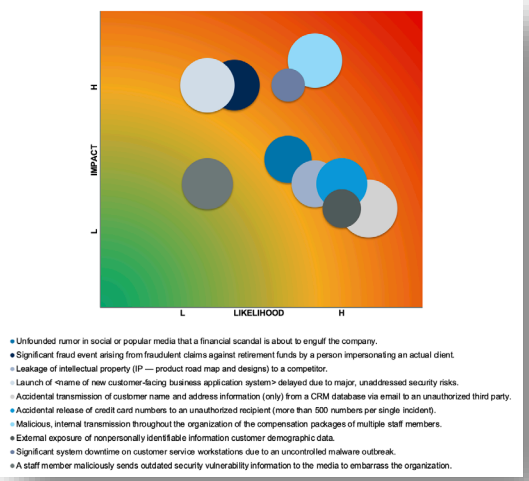
	Почти нереально	Маловероятно	Возможно	Вероятно	Очень вероятно
Катастрофически	6	7	8	9	10
Значительно	5	6	7	8	9
Умеренно	4	5	6	7	8
Незначительно	3	4	5	6	7
Несущественно	2	3	4	5	6
	Принять (уровень = 2,3)	Мониторить (уровень = 4,5)	Управлять (уровень = 6)	Избежать / разрулить (уровень = 7)	Немедленно избежать / разрулить (уровень = 8, 9, 10)

БИЗНЕС БЕЗ ОПАСНОСТИ

Как обычно измеряют риски/угрозы ИБ?

Трехфакторная оценка

Risk	Likelihood	Impact	Cost of Treatment ($)
Significant fraud event arising from fraudulent claims against retirement funds by a person impersonating an actual client.	4	8	7
Significant system downtime on customer service workstations due to an uncontrolled malware outbreak.	6	8	3
Leakage of intellectual property (IP — product road map and designs) to a competitor.	7	4	6
Launch of <name of new customer-facing business application system> delayed due to major, unaddressed security risks.	3	8	8
Unfounded rumor in social or popular media that a financial scandal is about to engulf the company.	6	5	6
Accidental release of credit card numbers to an unauthorized recipient (more than 500 numbers per single incident).	8	4	7
Malicious, internal transmission throughout the organization of the compensation packages of multiple staff members.	7	9	8
External exposure of nonpersonally identifiable information customer demographic data.	8	3	4
A staff member maliciously sends outdated security vulnerability information to the media to embarrass the organization.	3	4	7
Accidental transmission of customer name and address information (only) from a CRM database via email to an unauthorized third party.	9	3	9



* - вероятность лучше заменить на частоту

** - стоимость защитных мер опирается на расчет TCO

Источник: Gartner

БЕЗ БИЗНЕС ОПАСНОСТИ

Пример инструмента расчета риска: BITS

BITS KEY RISK MEASUREMENT TOOL FOR INFORMATION SECURITY OPERATIONAL RISKS

ISO Domain Reference	Basel Loss Category for Operational Risk	Threat Event	Vulnerability	Security Control	Likelihood of Threat (Input)	Degree to which Control is Implemented (Input)	Impact if Control is not Implemented (Input)	Control vs. Impact Score	Residual Risk Score
				analysis of new release functionality, testing and deployment schedules.				5	0,00
Communications and Operations Management	Business Disruption and System Failures	System software failure	Lack of documented incident management procedures.	Incident management procedures are in place and well documented including: actions to take in the event of information system failures or loss of service, denial of service attacks, errors resulting from incomplete or inaccurate business data, errors resulting from system or device misconfiguration, breaches or loss of confidentiality, recovery from specific incidents, gathering of evidence, documentation and recovery process.				5	0,00
Communications and Operations Management	Business Disruption and System Failures	System software failure	Incident response teams are unqualified.	Incident response teams have appropriate qualifications and necessary training.				5	0,00
Communications and Operations Management	Business Disruption and System Failures	System software failure	Incident response teams are not accessible in the event of an incident.	Incident response teams are accessible and available as needed.				5	0,00
Communications and Operations Management	Business Disruption and System Failures	System software failure	No ability to project future system capacity requirements.	Projection and planning for future system capacity requirements is performed.				5	0,00

Применяется финансовыми организациями для оценки рисков

БИЗНЕС БЕЗ ОПАСНОСТИ

Без трансляции оценки в описание смысла нет

Масштаб ущерба	Описание	Приемлемость
Незначительный	Ущерб, не затрагивающий функциональность объекта и стабильность его работы	Приемлем
Малый	Ущерб, не затрагивающий функциональность объекта и стабильность его работы	Приемлем
Средний	Ущерб, затрагивающий часть (не все) целевые функции объекта	Приемлем в отдельных случаях
Значительный	Ущерб, затрагивающий все целевые функции объекта с возможностью восстановления	Не приемлем
Критичный	Ущерб, затрагивающий часть все целевые функции объекта без возможности восстановления	Не приемлем

Чуть больше конкретики

Степень влияния	RTO	Процессы
Высокая	12 часов	Взаиморасчеты
	24 часов	Подача обязательной отчетности
Средняя	25–72 часа	Обработка финансовых транзакций Закрытие периода Консолидация Казначейские операции
Низкая	3–5 дней	Мониторинг цен
	1–5 недель	Налоговое администрирование и отчетность Комплайенс Управленческая отчетность

Реальный пример финансовой организации

Время		Уровень тяжести последствий	Последствия негативного события, повлекшего выход из строя используемой информационной системы
Длительность простоя ИС	Наступление негативного события		
Информационная система			
1 час	утро (до 12-00)	0	Практически нет влияния на процессы
	день (до 18-00)	3	Задержки в обработке документов. Клиентский негатив ввиду задержки обработки документов (далее - везде)
	вечер (до 24-00)	3	Неадекватный контроль (задержка расчета СЧА – базы контроля). Проблемы с выявлением нарушений и обработкой данных об устранении ранее совершенных и уведомлением Банка России
12 часов	утро (до 12-00)	2	Невозможность предоставления первичных документов клиентом. Невозможность предоставления отчетности в Банк России (ежедневная/ежемесячная). Отсутствие возможности согласования текущих операций клиента и операций предыдущего дня
	день (до 18-00)	2	Смещение времени обработки операций, проблемы со сверкой (Т-) и проведением согласований операций за предыдущий день. Риски несвоевременного выставления нарушений и направления уведомлений об устранении
	вечер (до 24-00)	2	Неадекватный контроль (задержка расчета СЧА). Проблемы с выявлением нарушений и обработкой данных об устранении ранее совершенных и уведомлением Банка России
1 сутки	утро (до 12-00)	1	Невозможность предоставления первичных документов клиентом. Невозможность предоставления отчетности в Банк России (ежедневная/ежемесячная). Отсутствие возможности согласования операций клиента и операций предыдущих дней
	день (до 18-00)	1	Смещение времени обработки операций, нарушение ежедневности сверки, отсутствие возможности проведения согласования операций. Несвоевременное выставление нарушений и уведомлений об устранении.
	вечер (до 24-00)	1	Неадекватный контроль (задержка расчета СЧА). Проблемы с выявлением нарушений и обработкой данных об устранении ранее совершенных и уведомлением Банка России
Более суток		1	Лицензионный риск (неисполнение лицензируемого вида деятельности)

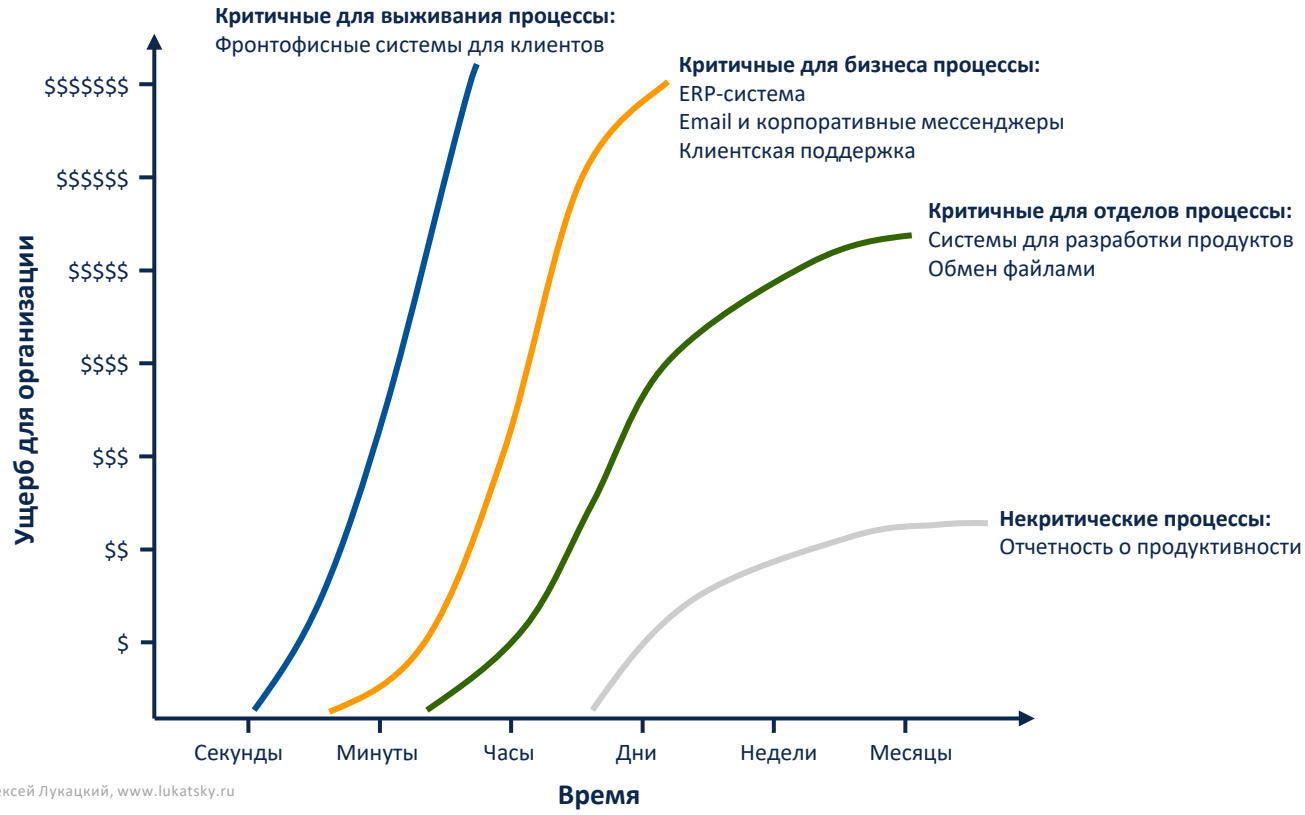
Недостатки качественной оценки

- Зависимость от квалификации эксперта / экспертов
- Зависимость от доверия к эксперту
- Влияние на мнение экспертов заинтересованными лицами
- Невозможность провести оценку для редких событий
- Отсутствие достаточного числа экспертов
- Психология восприятия рисков

Как правильно?

- Классифицировать информационные системы по степени их критичности
  - Зависит от бизнеса
- Определить возможные негативные последствия
  - Разные формы негативных последствий
- Оценить размер ущерба
  - Разные способы оценки ущерба
- Ранжировать ущерб
  - Обычно по трех- или пяти-балльной шкале

Разные системы имеют разную критичность и негативные последствия



Критичность различных информационных систем

БИЗНЕС БЕЗ ОПАСНОСТИ

Примеры негативных последствий

Из методики оценки угроз ФСТЭК

- Отсутствие доступа к государственной услуге
- Нарушение доступа к сайту ФОИВ
- Хищение денежных средств
- Отключение системы противоаварийной автоматики
- Нарушение работы рентгенографической установки
- Отключение системы управления транспортом

К чему может привести реализация угроз?

У ИБшников слабая фантазия в этом вопросе – привлекайте представителей бизнес-подразделений

- Нарушение прав граждан
- Возникновение ущерба в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности государства
- Возникновение финансовых, производственных, репутационных или иных рисков (видов ущерба) для обладателя информации, оператора

Как оценить ущерб/риски для ПДн?

https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

- Кейс: выплата зарплаты
- Кейс: рекрутинг
- Кейс: оценка персонала
- Кейс: заказ и доставка товаров
- Кейс: маркетинг и реклама
- Кейс: предоставление услуг
- Кейс: контроль доступа
- Кейс: видеонаблюдение
- Кейс: медицинские услуги и телемедицина
- Кейс: дистанционное образование

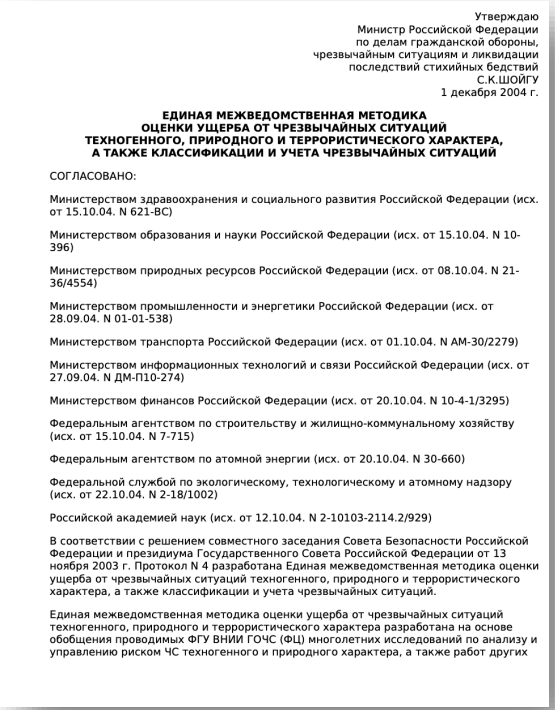
Систематизация последствий с точки зрения 6 свойств информации

Конфиденциальность	Целостность	Доступность	Подотчетность	Аутентичность	Достоверность
•Потеря общественного доверия •Снижение имиджа •Ответственность перед законом •Отрицательное влияние на политику организации •Создание угрозы безопасности персонала •Финансовые потери	•Принятие неправильных решений •Обман •Прерывание коммерческих операций •Потеря общественного доверия •Снижение имиджа •Финансовые потери •Ответственность перед законом	•Принятие неправильных решений •Неспособность выполнять важные поставленные задачи •Потеря общественного доверия •Снижение имиджа •Финансовые потери •Ответственность перед законом •Большие затраты на восстановление	•Манипулирование системой со стороны пользователей •Обман •Промышленный шпионаж •Неконтролируемые действия •Ложные обвинения •Ответственность перед законом	•Обман •Использование достоверных процессов с недостоверными данными •Манипулирование организацией извне •Промышленный шпионаж •Ложные обвинения •Ответственность перед законом	•Обман •Потеря доли рынка •Снижение мотивации в работе персонала •Ненадежные поставщики •Снижение доверия клиентов •Ответственность перед законом

Источник: ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Методы и средства обеспечения безопасности. Выбор защитных мер»

Какие методики оценки ущерба существуют?

- Единая межведомственная методика оценки ущерба от чрезвычайных ситуаций техногенного, природного и террористического характера, а также классификации и учета чрезвычайных ситуаций
  - Согласовано Минздравом, Минобрнауки, Минпромторгом, Минцифрой, Минтрансом, Минфином, Росатомом, Ростехнадзором, Минэнерго и т.п.



Утверждаю
Министр Российской Федерации
по делам гражданской обороны,
чрезвычайным ситуациям и ликвидации
последствий стихийных бедствий
С.К.ШОЙГУ
1 декабря 2004 г.

**ЕДИНАЯ МЕЖВЕДОМСТВЕННАЯ МЕТОДИКА
ОЦЕНКИ УЩЕРБА ОТ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ
ТЕХНОГЕННОГО, ПРИРОДНОГО И ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА,
А ТАКЖЕ КЛАССИФИКАЦИИ И УЧЕТА ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ**

СОГЛАСОВАНО:

Министерством здравоохранения и социального развития Российской Федерации (исх. от 15.10.04. N 621-ВС)

Министерством образования и науки Российской Федерации (исх. от 15.10.04. N 10-396)

Министерством природных ресурсов Российской Федерации (исх. от 08.10.04. N 21-36/4554)

Министерством промышленности и энергетики Российской Федерации (исх. от 28.09.04. N 01-01-538)

Министерством транспорта Российской Федерации (исх. от 01.10.04. N АМ-30/2279)

Министерством информационных технологий и связи Российской Федерации (исх. от 27.09.04. N ДМ-П10-274)

Министерством финансов Российской Федерации (исх. от 20.10.04. N 10-4-1/3295)

Федеральным агентством по строительству и жилищно-коммунальному хозяйству (исх. от 15.10.04. N 7-715)

Федеральным агентством по атомной энергии (исх. от 20.10.04. N 30-660)

Федеральной службой по экологическому, технологическому и атомному надзору (исх. от 22.10.04. N 2-18/1002)

Российской академией наук (исх. от 12.10.04. N 2-10103-2114.2/929)

В соответствии с решением совместного заседания Совета Безопасности Российской Федерации и президиума Государственного Совета Российской Федерации от 13 ноября 2003 г. Протокол N 4 разработана Единая межведомственная методика оценки ущерба от чрезвычайных ситуаций техногенного, природного и террористического характера, а также классификации и учета чрезвычайных ситуаций.

Единая межведомственная методика оценки ущерба от чрезвычайных ситуаций техногенного, природного и террористического характера разработана на основе обобщения проводимых ФГУ ВНИИ ГОЧС (ФЦ) многолетних исследований по анализу и управлению риском ЧС техногенного и природного характера, а также работ других

Ущерб принимает разные формы

- Все без исключения ЧС техногенного, природного и террористического характера наносят или могут нанести ущерб интересам личности, общества и государства, выражающийся в следующих видах ущерба:
  - ущерб жизни и здоровью населения
  - экономический ущерб, связанный с материальными потерями, вызванными повреждениями и разрушениями производственных и непроизводственных объектов, нарушением их функционирования, затратами на предупреждение и ликвидацию ЧС
  - экологический ущерб (ущерб природной среде)
  - другие виды ущерба, в том числе ущерб культурным ценностям, моральный ущерб и т.д.
- Это принципиально разные виды ущерба, несводимые друг к другу и подлежащие раздельному учету

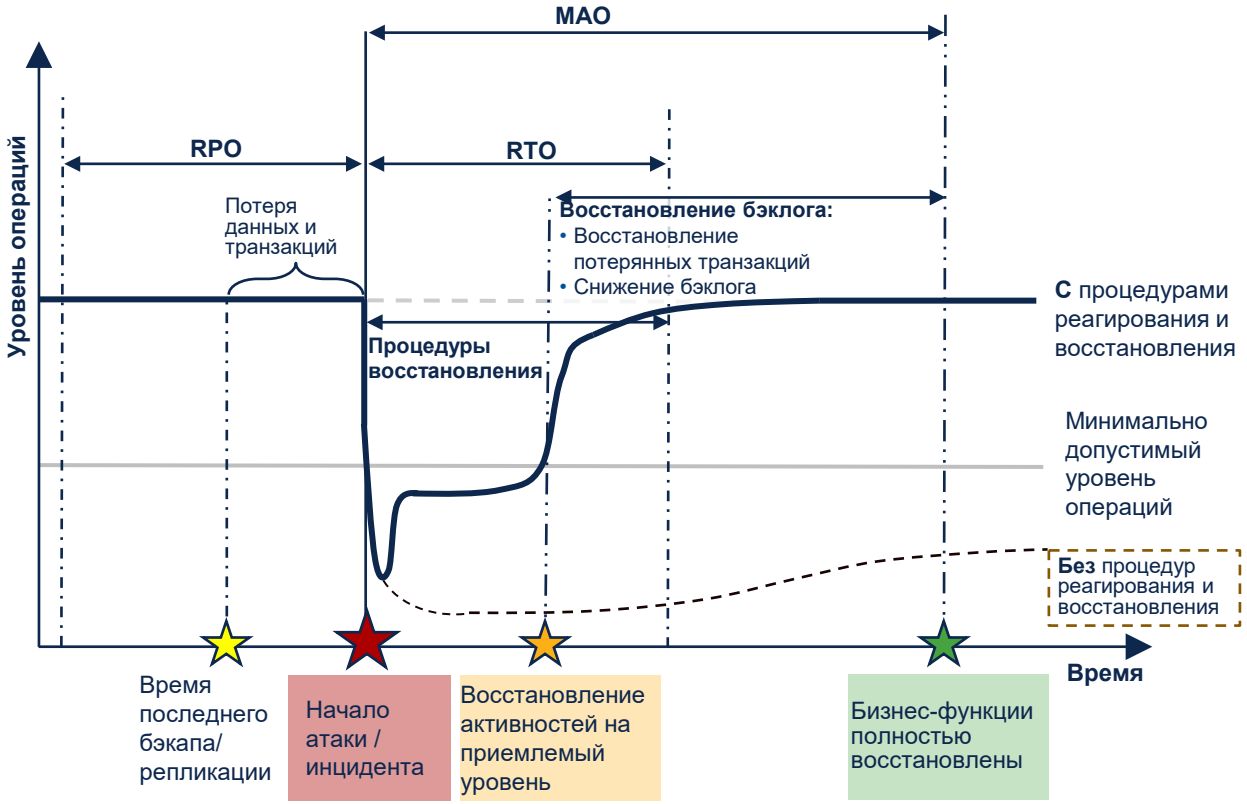
Вторичность экономического ущерба

- Деятельность по определению экономического ущерба вторична по отношению к определению физического ущерба от ЧС
  - Это означает, что прежде чем приступить к экономической оценке ущерба от ЧС, должна быть проведена работа по определению разрушений и иных потерь в натуральных (физических и иных) измерителях, т.е. определен физический ущерб от ЧС
- При определении экономического ущерба:
  - осуществляется переход (пересчет) показателей физического ущерба в стоимостные (денежные) измерители
  - прямо или косвенно воспроизводятся (моделируются) экономические процессы функционирования объектов экономики и социальной инфраструктуры применительно к условиям ЧС

Нюансы расчета экономического ущерба

- При определении экономического ущерба выделяется фактический (расчетный) экономический ущерб, как правило, исчисляемый в годовом измерении и выражаемый в ценах и расценках предыдущего года
- Такое «запаздывание» объясняется спецификой статистической отчетности
- Принимается годовой лаг в расчетах ущерба, он принят в качестве базового

Длительность инцидента ИБ с точки зрения бизнеса



БИЗНЕС БЕЗ ОПАСНОСТИ

Длительность последствий зависит от типа актива

Но годовой период признан базовым, в том числе и в ПП-127 по категорированию объектов КИИ

Поэтому так важно начать с классификации информационных систем

Прямой и косвенный ущерб

$$U = U_p + A * U_k$$

- A - коэффициент приведения разновременных затрат (коэффициент дисконтирования)
  - Именно тут важно учитывать длительность негативных последствий
- U - экономический ущерб от инцидента
- U_p - прямой экономический ущерб
- U_k - косвенный экономический ущерб

Проведите декомпозицию!

Для этого надо неплохо разбираться в бизнесе, который вы защищаете (в деятельности своего предприятия)

А если актив не завязан на генерацию финансовых средств, но важен для бизнеса?

- Детальная оценка стоимости атаки включает в себя:
  - Стоимость простоя атакуемого актива (потеря продуктивности)
  - Стоимость восстановления атакуемого актива, включая привлечение внешних сил
  - Дополнительные затраты (штрафы, неустойки, репутация, судебные тяжбы, уход клиентов и т.п.)
  - Потенциальные сбережения (например, электричество или Интернет)

Минимальные исходные данные для расчета

- Время простоя вследствие атаки
- Время восстановления после атаки
- Время повторного ввода потерянной информации
- Зарплата обслуживающего персонала
- Зарплата сотрудников атакованного узла или сегмента
- Численность обслуживающего персонала
- Численность сотрудников атакованного узла/сегмента
- Объем продаж, выполненных с помощью атакованного узла или сегмента
- Стоимость замены оборудования или запасных частей

Какие потери несет бизнес?

- Потери интеллектуальной собственности
  - Ноу-хау, патенты, списки клиентов, условия договоров
- Юридические потери
  - Штрафы и досудебные урегулирования
- Потери «собственности»
  - Курс акций, перехват управления, вывод из строя, информация, приводящая к задержкам в выпуске продукции или услуг, кража денег со счета
- Репутационные потери
  - Снижение лояльности → снижение ARPU, уход клиентов, негативные отзывы в прессе

Какие потери несет бизнес?

- Потери времени (простои) на восстановление и расследование
- Административные затраты на восстановление, взаимодействие с клиентами и регуляторами, возврат в предатакованное состояние
- Операционные
- Вред окружающей среде
- Ущерб жизни и здоровью
- Получение конкурентами преимуществ
- Подрыв доверия инвесторов и акционеров

А как считать эти потери (хотя бы некоторые)?

Помимо единой методики оценки ущерба от ЧС

- Рекомендации по оценке показателей критериев экономической значимости объектов КИИ
  - ФСТЭК
- Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения (Версия 1.0)
  - Минздравсоцразвития
  - Оценка вреда жизни и здоровью, отсутствия доступа к услуге, нарушение функционирования сайта, ущерб бюджету РФ, воздействие на окружающую среду…

БИЗНЕС БЕЗ ОПАСНОСТИ

А как считать эти потери (хотя бы некоторые)?

Помимо единой методики оценки ущерба от ЧС

- Методические рекомендации по определению и категорированию объектов КИИ топливно-энергетического комплекса
- Методические рекомендации по категорированию объектов КИИ, принадлежащих субъектам КИИ, функционирующим в сфере связи

А какой косвенный ущерб может быть?

Продуктивность	• Простои • Ухудшение психологического климата
Реагирование	• Расследование инцидента • PR-активность
Замена	• Замена оборудования • Повторный ввод информации
Штрафы	• Судебные издержки, досудебное урегулирование • Приостановление деятельности
Конкуренты	• Ноу-хау, государственная, коммерческая тайна • Отток клиентов, обгон со стороны конкурента
Репутация	• Гудвил • Снижение капитализации, курса акций

БИЗНЕС БЕЗ ОПАСНОСТИ

Даже если посчитать рублем, то ущерб может быть разный

- Не любой финансовый ущерб значим для организации или ее подразделений или бизнес-проектов
- Важно ранжировать весь ущерб, разбив его на диапазоны от не незначительного до катастрофического (риск-аппетит)
- Определяется менеджментом организации

	Несущественно	Незначительно	Умеренно	Значительно	Катастрофически
Финансовый ущерб на более чем **Y** миллионов рублей	₽1M	₽5M	₽10M	₽50M	₽100M

Ранжирование при иных формах ущерба

	Несущественно	Незначительно	Умеренно	Значительно	Катастрофически
Перебой в работе для более чем **X** заказчиков	10 заказчиков	100 заказчиков	500 заказчиков	1000 заказчиков	5000 заказчиков
Прерывание бизнес операций на **Z** часов	1 час	4 часа	8 часов	2 дня	5 дней
Нанесение вреда жизни и здоровью **A** человек	0 человек	0 человек	1 человек	10 человек	50 человек
Утечка данных **B** заказчиков	100 заказчиков	1000 заказчиков	5000 заказчиков	10000 заказчиков	100000 заказчиков
Отток **C** заказчиков	5 заказчиков	10 заказчиков	25 заказчиков	50 заказчиков	100 заказчиков
Потеря доли рынка на **D**%	0%	0%	1%	3%	7%
Снижение продуктивности на **E**%	0%	1%	3%	5%	10%

Специфичные отраслевые метрики

	Несущественно	Незначительно	Умеренно	Значительно	Катастрофически
Снижение мощности электрогене-рации на **F** мегаватт	Снижение мощности допустимо	Снижение мощности допустимо	100 МВт	1000 МВт	10000 МВт

	Несущественно	Незначительно	Умеренно	Значительно	Катастрофически
Публикация в СМИ	Отсутствуют	В местных потребительских печатных изданиях	По местному ТВ или в местных отраслевых печатных изданиях	По национальному ТВ или в национальных потребительских печатных изданиях	Выделенная передачи или репортаж по национальному ТВ или в национальных отраслевых печатных изданиях

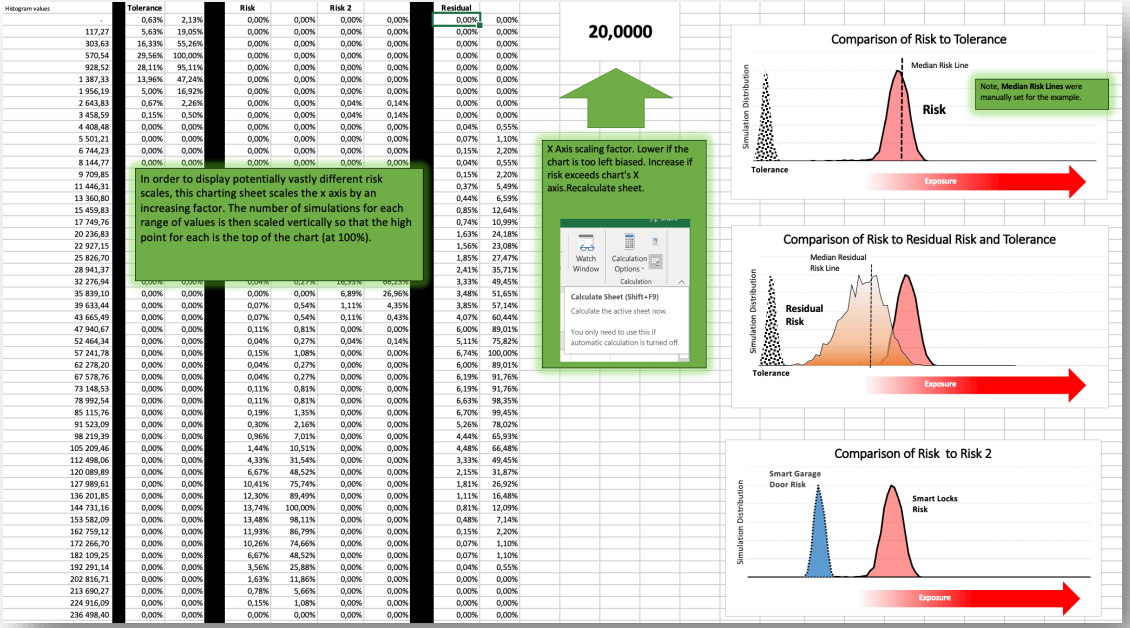
Разные виды и градации ущерба для банка

- ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности»
- 6 видов ущерба
  - Финансовый
  - Репутационный
  - Стратегический
  - Правовой
  - Операционной
  - Безопасность
- 9 градаций негативных последствий

Рейтинг		Описание	Репутация	Операционный	Безопасность	Правовой	Финансовый	Стратегический
НИЗКИЙ	1	пренебрежимо малое			Локальный пароль к не секретным данным раскрыт, но не использован		<$100	
	2	очень незначительное	Нападки на банковскую систему по местному радио и в местной прессе	Незначительное количество эксплуатационных проблем, не оказывающих воздействие на клиентов	Локальный пароль к секретным данным раскрыт, но не использован	Правовые ответы от участника клиринга не выполняются во временной период, определенный законом	~$1 000	
	3	незначительное	"Стандартные" язвительные высказывания в национальной прессе или размещенные в Интернете о банковской системе, например, письмо читателя	Временное невыполнение обслуживания (~1 ч.) для одного члена системы; проблемы, оказывающие ограниченное влияние на клиентов	Утечка или компрометация незначительного количества текущей информации	Идентифицирована поправимая возможность несоответствия	~$5 000	Политики или стандарты не поддерживаются
СРЕДНИЙ	4	заметное	Внимание национальной прессы или радио, например, плохой отзыв в DD схеме	Эксплуатационные проблемы, оказывающие воздействие на весь клиринг	Злоупотребление законными привилегиями доступа	Неспособность предоставить данные, требуемые законом, например, согласно закону Сэрбэйнс-Оксли	~$20 000	
СРЕДНИЙ	5	существенное	Серьезная критическая статья в прессе или документальная передача по радио или по телевизору, склонная рассматриваться как исходящая из заслуживающего доверия источника	Временное невыполнение обслуживания для многих членов системы или длительное невыполнение обслуживания (до целого дня) для одного члена системы; существенное воздействие на клиентов	Логическое или физическое проникновение в операционные системы одного или более членов системы; например, вредоносный вирус, причинивший некоторый ущерб	Правовое вмешательство, иск не удовлетворен	~$100 000	Политики или стандарты не существуют
	6	очень существенное	Публичная критика со стороны регулятивного или отраслевого органа	Член системы не способен работать с клирингом	Успешное мошенничество мелкого - среднего масштаба	Начало полицейского или регулятивного расследования; регулятивное вмешательство, иск удовлетворен	~$1 000 000	
	7	большое	Ведущая новость во многих газетах и/или в основных телевизионных новостях	Невыполнение обслуживания для многих членов системы в критическое время дня (15:00, пятница)	Успешное мошенничество крупного размера; операционные данные или системы контроля скомпрометированы	Судебное преследование, возбужденное против клиринговой палаты (неуспешное)	~$10 000 000	Управленческий контроль скомпрометирован
ВЫСОКИЙ	8	очень большое	Государственное вмешательство или сравнимые политические последствия	Невыполнение клиринга в течение всего рабочего дня	Клиринговая система взломана и серьезно скомпрометирована	Судебное преследование, возбужденное против клиринговой палаты (успешное)	~$100 000 000	
	9	катастрофическое	Широкое освещение прессой и телевидением, полная потеря доверия со стороны публики и членов системы	Полное невыполнение обслуживания в течение нескольких дней/недель	Клиринговая палата или ее криптографические системы полностью скомпрометированы, мошенничество крупного масштаба без известной оценки	Систематическое и умышленное несоблюдение закона руководством высшего уровня	~ $1 000 000 000	Будущее существование клиринговой палаты под сомнением; платежная индустрия скомпрометирована

А как учесть вероятностную сущность будущего ущерба?

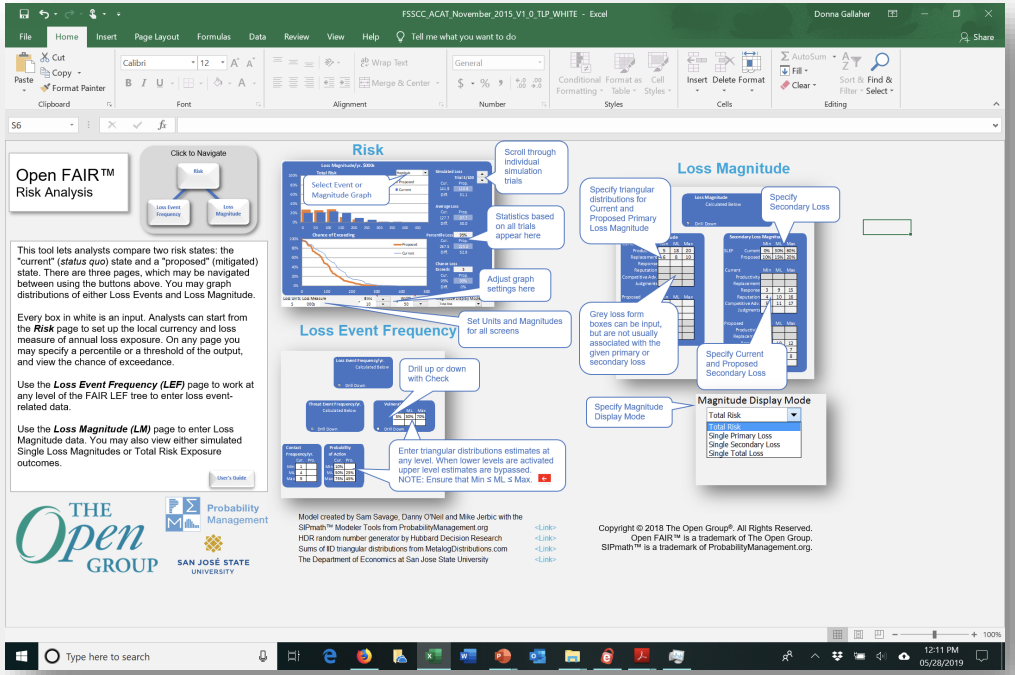
- Оценка ущерба обычно базируется на прошлых периодах
  - Метод Annual Loss Expectancy (ALE)
- Как посчитать будущий ущерб, учитывая его непредсказуемость?
- Метод Монте-Карло
  - Тысячи экспериментов



Источник: FAIR Privacy Calculator v2.12

Пример инструмента расчета риска: Open FAIR

- Калькулятор Open FAIR базируется на методе оценки рисков FAIR и позволяет оценить не только частоту рисков, но и ущерб
  - Прямой и непрямой
  - Эмуляция 10000 экспериментов и получение распределение размеров вероятных ущербов



Ценность информации

Защита не должна быть дороже защищаемой информации, но как считать стоимость информации?

- Активы бывают материальные и нематериальные
- Материальные активы оцениваются обычно на основе стоимости их замены или восстановления
- Аналогичным образом часто оценивается и программное обеспечение
- Ценность информации и иных нематериальных активов определяется либо экспертным способом (метод Дельфи) или с помощью специальных методик

Нематериальные активы – это то, что и требует в реальности защиты

- Патенты, изобретения, технологии…
- Авторские права
- Деловая репутация
- Фирменные знаки и наименования
- Документированные консультации
- Торговые марки
- ПО, обособленное по «железа»
- Права на эксплуатацию
- Лицензии
- И т.д.

БЕЗ ОПАСНОСТИ БИЗНЕС

Виды стоимости нематериального актива

Вид стоимости	Определение
Стоимость обмена	Вероятная цена продажи, когда условия обмена известны обеим сторонам и сделка считается взаимовыгодной
Обоснованная рыночная стоимость	Наиболее вероятная цена, по которой объект оценки переходит из рук одного продавца в руки другого на открытом рынке и добровольно
Стоимость использования	Стоимость объекта оценки в представлении конкретного пользователя и с учетом его ограничений
Ликвидационная стоимость	Стоимость объекта оценки при вынужденной продаже, банкротстве
Стоимость замещения	Наименьшая стоимость эквивалентного объекта оценки

Методы оценки НМА

- У каждого метода есть своя область применения, свои достоинства и недостатки

Рыночный	Затратный	Доходный
• Метод сравнения продаж аналогичных объектов оценки	• Метод стоимости замещения • Метод восстановительной стоимости • Метод исходных затрат	• Метод расчета роялти • Метод исключения ставки роялти • Метод DCF • Метод прямой капитализации • Экспресс-оценка • Метод избыточной прибыли • Метод по правилу 25% • Экспертные методы

В чем сложность расчета стоимости информации?

Помимо нежелания влезать в это la merde ☺

- Изменчивость стоимости одного и того же актива
- Разные методы подсчета стоимости одного и того же актива
- Бизнес должен хотеть считать стоимость информации
- Негативное отношение налоговой к этому методу «ухода от налогов»

БИЗНЕС БЕЗ ОПАСНОСТИ

Сложности расчета негативных последствий

Экспертная оценка

Последствия в ИБ-терминах

Понимание бизнес-процессов

Отсутствие исходных данных

Взаимодействие с бизнесом

Нематериальные активы

Резюмируя

Не забывая про необходимость оценки еще и вероятности риска

- Без понимания ущерба от реализации рисков (угроз) невозможно эффективно заниматься кибербезопасностью
- Ущерб может быть не только финансовым
- За счет декомпозиции ущерб может быть посчитан достаточно точно
- Качественная оценка тоже возможна, если все градации точно объяснены с точки зрения бизнеса

Вопросы?

Может быть в этом году мы попробуем иную стратегию кибербезопасности?

БИЗНЕС БЕЗ ОПАСНОСТИ

alexey@lukatsky.ru