Управление рисками информационной безопасности

Агеева Елена
Ведущий консультант по информационной безопасности

Проверка связи

Если у вас нет звука:

- убедитесь, что на вашем устройстве и на колонках включён звук
- обновите страницу вебинара (или закройте страницу и заново присоединитесь к вебинару)
- откройте вебинар в другом браузере
- перезагрузите компьютер (ноутбук) и заново попытайтесь зайти

Поставьте в чат:

\+ если меня видно и слышно

\– если нет

Елена Агеева

О спикере:

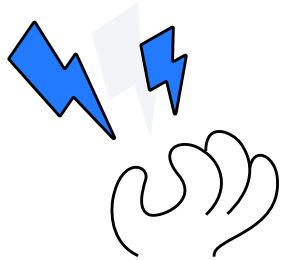
- ведущий консультант по информационной безопасности
- более 5 лет опыта в сфере ИБ
- основные направления работы: оценка рисков ИБ, защита от утечек конфиденциальной информации, защита персональных данных
- и коммерческой тайны, экспертный консалтинг ИБ

Правила участия

1. Приготовьте блокнот и ручку, чтобы записывать важные мысли и идеи
2. Продолжительность вебинара — 80 минут
3. Вы можете писать вопросы в чате

Вспомним материалы лекций

1. Узнали, зачем компаниям нужно управлять рисками ИБ
2. Разобрались, какие существуют стандарты по оценке рисков ИБ и когда необходимо соответствие им
3. Поняли, как осуществлять оценку и анализ рисков ИБ
4. Рассмотрели, какие документы являются результатами управления рисками



Приведите пример риска из повседневной жизни

Вспоминаем материалы лекции

Вопрос: что такое риск ИБ?

Вспоминаем материалы лекции

Вопрос: что такое риск ИБ?

Ответ: возможность реализации угрозы из-за уязвимости информационного актива

Вспоминаем материалы лекции

Вопрос: зачем компании нужно управление рисками ИБ?

Вспоминаем материалы лекции

Вопрос: зачем компании нужно управление рисками ИБ?

Ответ:

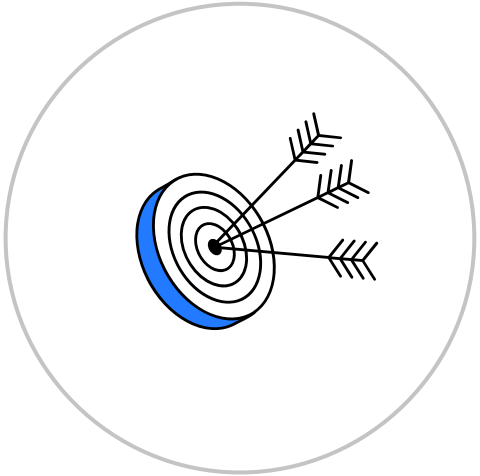
1. Чтобы приоритизировать мероприятия по защите конфиденциальной информации

2. Помогает определить, какие риски недопустимы настолько, что необходимо принять меры по их снижению или недопущению

Ваши вопросы?

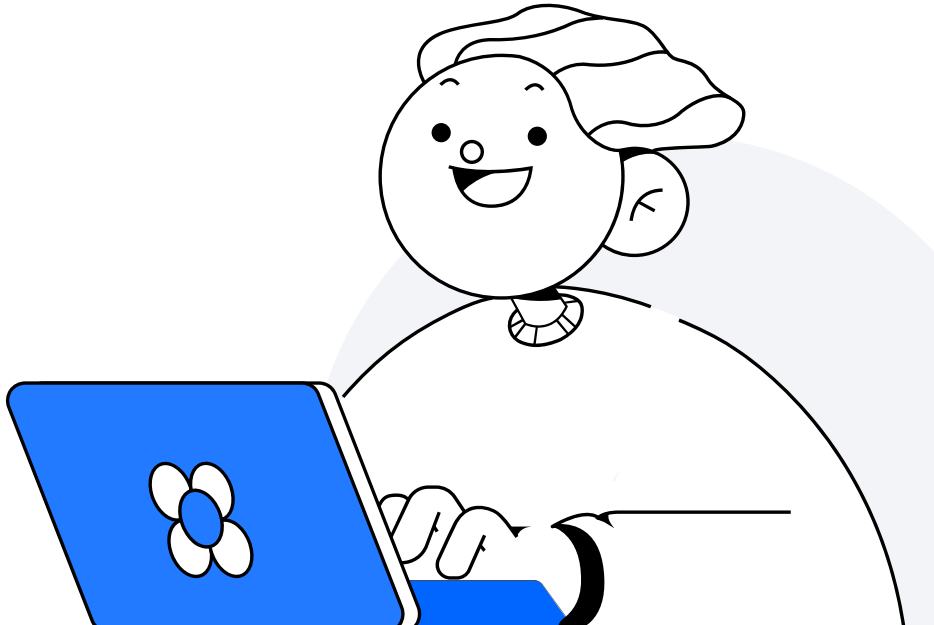
Цели занятия

- Разобрать, что необходимо сделать до начала процесса управления рисками
- Узнать, что такое качественная и количественная оценка рисков ИБ
- Понять, чем отличаются внутренние и внешние факторы контекста организации
- Рассмотреть на примерах процесс проведения оценки рисков ИБ



План занятия

1. Подготовка к управлению рисками информационной безопасности
2. Оценка рисков информационной безопасности
3. Итоги



Подготовка к управлению рисками информационной безопасности

1

До начала процесса управления рисками

Необходимо определить

1. В соответствии с какими лучшими практиками и требованиями будет проводиться процесс
2. Кто принимает участие в процессе и какая у них ответственность
3. Контекст компании, область применения процесса управления рисками
4. Метод проведения оценки рисков: качественная или количественная оценка

Методологии оценки рисков ИБ

1

ISO/IEC 27005 Information Security Risk Management[1]

Лучшая практика / Требование

2

ISO 31000 Risk Management[2]

Лучшая практика

3

NIST SP 800-30 Guide for Conducting Risk Assessments

Лучшая практика

4

Положение Банка России № 716-П

«О требованиях к системе управления операционными рисками в кредитной организации и банковской группе»

Требование

1 Аналог — ГОСТ Р ИСО/МЭК 27005 Менеджмент риска информационной безопасности
2 Аналог — ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

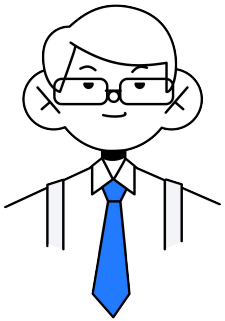
Методологии оценки рисков ИБ

Итоговый выбор методов зависит от:

- опыта специалистов, проводящих оценку рисков
- необходимости соблюдения требований и более подходящей модели управления рисками для конкретной компании

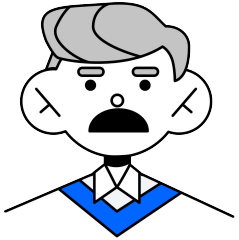
Управление рисками может строиться сразу на нескольких стандартах.
Также могут использоваться те, которые не приведены в рамках вебинара

Кто участвует



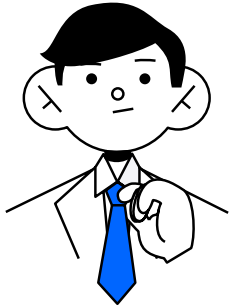
Менеджер по управлению рисками ИБ

- Отвечает за процесс
- Собирает необходимую информацию
- Проводит оценку рисков
- Контролирует выполнение процесса
- Мониторит риски



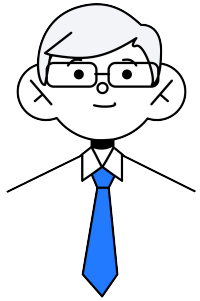
Руководство компании

- Согласовывает результат
- Принимает окончательное решение в случае спорных ситуаций



Специалисты по ИБ

- Помогают менеджеру
- Обсуждают принятие решений в рамках оценки рисков



Работники структурных подразделений

- Делятся с менеджером информацией, необходимой для оценки рисков

Контекст компании*

Внешние факторы

1. Необходимость соблюдения законодательства РФ в области защиты персональных данных
2. Необходимость соблюдения отраслевых требований
3. Невозможность продления лицензий на некоторые операционные системы

Внутренние факторы

1. Недостаток персонала, осуществляющего производственные процессы
2. Отсутствие персонала, администрирующего средства защиты информации
3. Сложность ИТ-инфраструктуры

* Контекст компании — комбинация внутренних и внешних факторов, которые могут оказать влияние на подход организации к разработке и достижению своих целей

Приведите другие примеры внешних и внутренних факторов контекста организации

Управление рисками ИБ. Область применения

Все информационные активы компании

Все критичные информационные активы компании

Информационные активы, участвующие в поддержке ИТ-инфраструктуры компании

Информационные активы, участвующие в производстве товаров

Информационные активы, участвующие в процессе обработки персональных данных

Информационные активы, участвующие в поддержке критической информационной инфраструктуры

Информационные активы, участвующие в обработке коммерческой тайны

Методы оценки рисков

Качественная оценка

Определение риска
с помощью неточных величин:

- низкий
- средний
- высокий

Плюсы

- не требует точного определения стоимости ущерба
- интуитивно понятная оценка

Минусы

- неточность определения величины может привести к некорректной оценке риска — он может быть переоценён или недооценён

Методы оценки рисков

Количественная оценка

Определение риска посредством точной величины.

Например, в результате простоя системы в течение 2 часов компания потеряет 1 млн рублей

Плюсы

- руководство компании лучше понимает реальный ущерб от того или иного риска, сравнивая его затратами на предотвращение или минимизацию риска

Минусы

- сложно определить точное количество денежных потерь от того или иного риска

Количественная оценка рисков. Примеры

Зарплата специалиастов, работающих над восстановлением системы

Количество специалистов, время восстановления системы, сверхурочные в случае простоя в нерабочее время

Зарплата специалистов, работающих над восстановлением данных, которые не успели сохраниться

Данные за последний час должны быть восстановлены вручную

Упущенная выгода

Умножить количество не совершивших покупки клиентов на среднюю стоимость одной покупки

Репутационные риски

Сколько клиентов больше не будут совершать покупки

Затраты на маркетинговые мероприятия

Которые направлены на возвращение клиентов

Приведите другие примеры составляющих, которые можно использовать в количественной оценке рисков ИБ

Выводы

1. Итоговый выбор методологии по оценке рисков ИБ зависит от специфики компании и опыта специалистов, которые проводят оценку
2. В процессе оценки участвуют: менеджер по управлению рисками ИБ, руководство компании, специалисты по ИБ и работники структурных подразделений компании
3. Контекст компании определяется внутренними и внешними факторами
4. Область применения управления рисками ИБ должна включать в себя все критичные для компании активы
5. Качественная оценка рисков легче в выполнении, однако количественная показывает более точные данные для принятия решений

Ваши вопросы?

Перерыв

5 минут

Оценка рисков информационной безопасности

2

Вспоминаем материалы лекции

Вопрос: что такое информационный актив?

Вспоминаем материалы лекции

Вопрос: что такое информационный актив?

Ответ: знания или данные, которые имеют потенциальную ценность для компании

Вспоминаем материалы лекции

Вопрос: какие документы должны появиться в компании после организации процесса управления рисками ИБ?

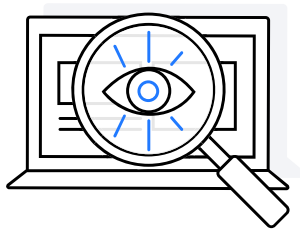
Вспоминаем материалы лекции

Вопрос: какие документы должны появиться в компании после организации процесса управления рисками ИБ?

Ответ:

- методика оценки рисков ИБ
- отчёт об оценке рисков ИБ
- план обработки рисков ИБ

Демонстрация проведения оценки рисков ИБ



Этапы проведения оценки рисков ИБ

- Задача оценки
- Внешние факторы
- Внутренние факторы
- Информационные активы
- Имеющиеся средства защиты информации
- Угрозы и уязвимости
- Отчёт об оценке рисков ИБ
- План обработки рисков ИБ

Вывод

Для оценки рисков ИБ необходимо заполнить отчёт об оценке рисков ИБ и план обработки рисков ИБ

Ваши вопросы?

Итоги занятия

1. Разобрали, что необходимо сделать до начала процесса управления рисками
2. Узнали, что такое качественная и количественная оценка рисков ИБ
3. Поняли, чем отличаются внутренние и внешние факторы контекста организации
4. Рассмотрели на примерах процесс проведения оценки рисков ИБ

Анонс следующего занятия

1. Воркшоп по оценке рисков ИБ

Управление рисками информационной безопасности

Агеева Елена
Ведущий консультант по информационной безопасности