Программная инженерия

Москва
2026

Лекция № 7. Оценка рисков

Основы кибербезопасности

Белявский Д.А.

Выбор организации

1 команда НЕ выбрала организацию

Чемпионы

Ведомость с результатами контрольных работ.
И список организаций по КОМАНДАМ

2 команды выбрали ОДИНАКОВУЮ организацию

Cherrypickme

Тимур и его команда

Самостоятельная работа по оценке рисков

1. Выбор организации
(здесь командная работа, одна организация на команду)
2. Выбор информационной системы
(тут индивидуально, повторов быть не может, уникально)
3. Рассчитываем «стоимость» информационной системы,
как СУММУ всех конкурсов по именно вашей ИС
4. Определение программного обеспечения
(5 видов ПО, вместе с версиями)

Самостоятельная работа по оценке рисков

4 Определяем уязвимости по каждому ПО (25 уязвимостей, по 5 уязвимостей на каждое ПО)

5 Для каждой уязвимости определяем уровень опасности и приводим к процентам (т.к. шкала 10-бальная, то делим на 10)

6 Из БДУ ФСТЭК выбираем угрозы и сопостовляем с каждой (!) уязвимостью из списка

7 Для каждой угрозы анализируем «источник угрозы» и определяем вероятность реализации угрозы по вашей шкале, например, «0%, 25%, 50%, 75%, 100%»

- БДУ ФСТЭК
- CVE MITRE
- Vulners

Самостоятельная работа по оценке рисков

8 Рассчитываем показатель (значение) риска по формуле риска, где в качестве цены потери используем «стоимость» ИС

$$R = P_{\text{угрозы}} \times P_{\text{уязвимости}} \times D$$

9 Ранжируем риски – сортируем от большего к меньшему значению риска

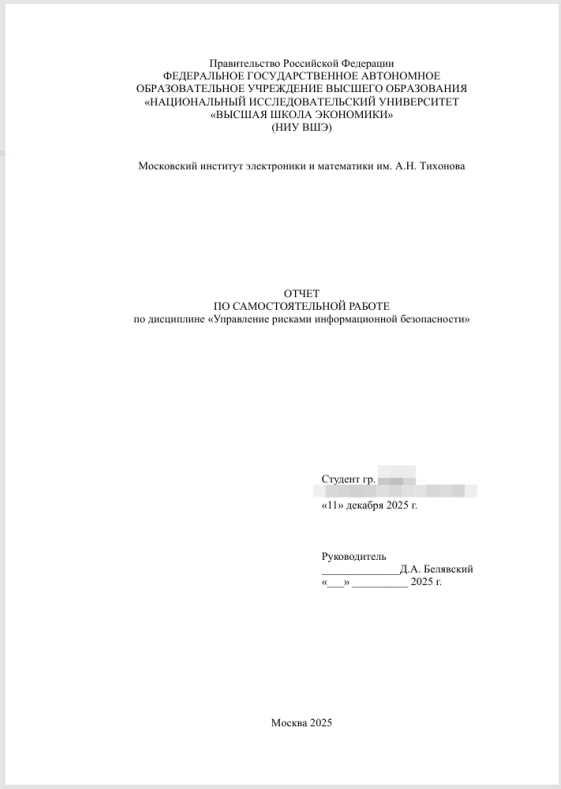
10 Анализируем риски на предмет их минимизации (сокращения)

Шаблон таблицы

Цена потери (ущерб) расцениваем как СТОИМОСТЬ всей информационной системы

Риск	Угроза, с помощью которой может быть реализована уязвимость	Программное обеспечение	Уязвимость (номер и описание)	$P_{уязвимости}$	$P_{угрозы}$	D	R
Риск доступа к защищаемым файлам с использованием обходного пути	УБИ.015 Угроза доступа к защищаемым файлам с использованием обходного пути **Источник угрозы:** Внешний нарушитель с низким потенциалом; Внутренний нарушитель с низким потенциалом	IBM AIX 7.2	BDU:2025-16251 Уязвимость операционных систем IBM AIX и IBM VIOS связана с ошибками инициализации. Эксплуатация уязвимости может позволить нарушителю получить доступ на запись произвольных файлов	= 7,4 / 10 = 74%	75%	15 401 522,33	8 547 844,89
Риск удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	УБИ.195 Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы **Источник угрозы:** Внешний нарушитель с высоким потенциалом	IBM AIX 7.2	BDU:2025-14676 Уязвимость сервера NIM операционной системы IBM AIX и IBM VIOS связана с некорректным управлением процессами. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольные команды	= 10 / 10 = 100%	25%	15 401 522,33	3 850 380,58

Оформление самостоятельной работы



Правительство Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

ОТЧЕТ
ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ
по дисциплине «Управление рисками информационной безопасности»

Студент гр.
«11» декабря 2025 г.

Руководитель
_____Д.А. Белявский
«___» _____ 2025 г.

Москва 2025

1. Электронный документ, формат PDF

2. Разделы документа:

   1. Организация и выбранная информационная система
   2. Программное обеспечение для ИС
   3. Таблица (одна) с расчетом рисков
   4. Анализ рисков (выводы)

Предоставление и защита работ

На семинаре

Команда готовит «общую» презентацию по организации

У каждого студента – 1 слайд по своей ИС с 2-мя максимальными рисками

Каждый студент выступает и объясняет, как рассчитал риски:
- что за ПО используется, найденные уязвимости
- как связал с угрозами
- почему именно эти 2 риска максимальны

Предоставление электронной версии работы

Срок предоставления документа с самостоятельной работой:
последний семинар 3-го модуля

Документы необходимо отправить на почту:
dbelyavskiy@hse.ru
В письме обязательно указываем:
- в теме: Фамилия Имя и группа
- в самом письме: Команда и выбранная ИС

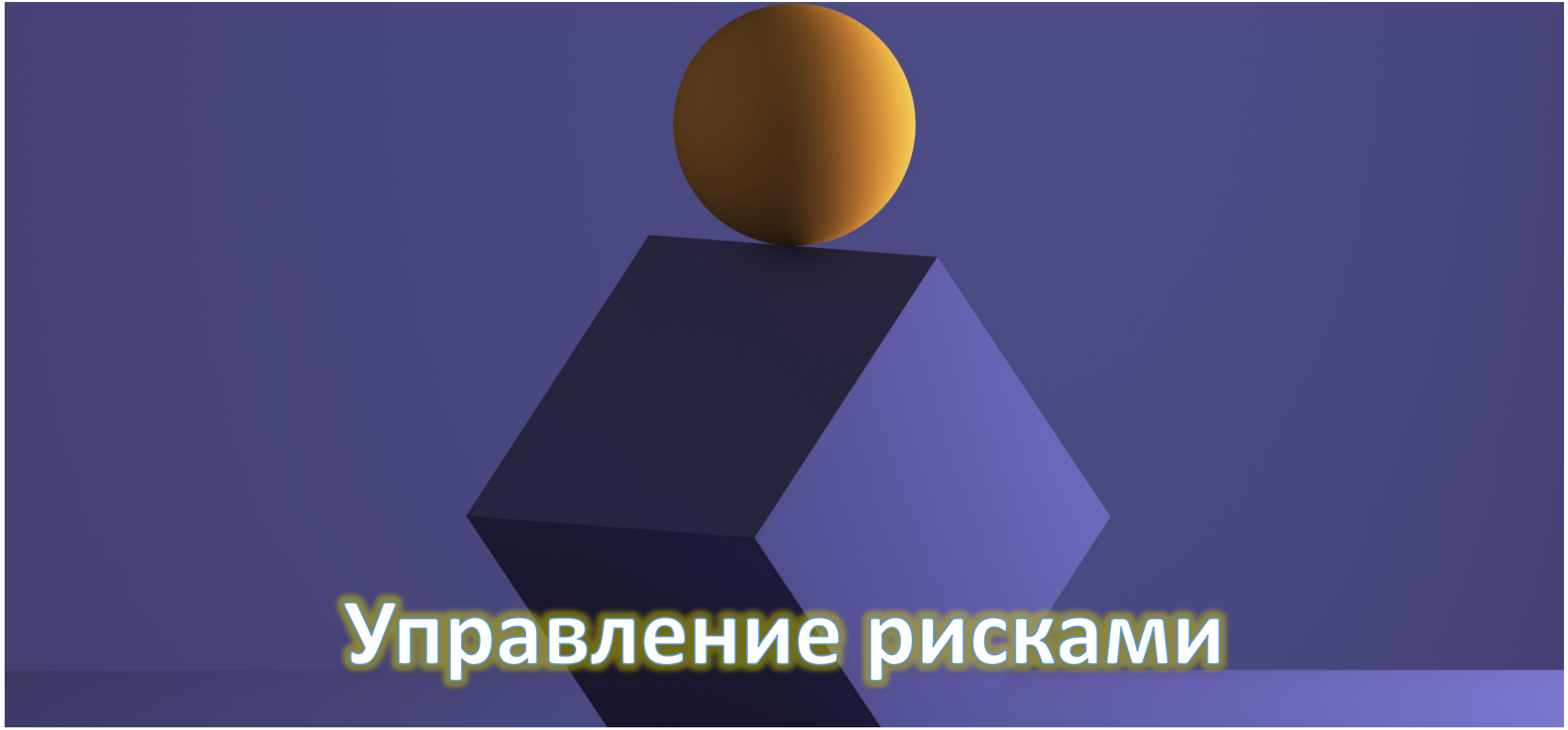
Защиту оценивает семинарист

По 10-бальной шкале → 40%

Работу оценивает лектор

По 10-бальной шкале → 60%

Оценка за работу


Управление рисками

Зачем нужно управлять рисками?

Суть мероприятий по управлению рисками состоит в том, чтобы
оценить их размер, обработать риски, выработать эффективные и экономичные ***меры снижения рисков***
а затем убедиться, что:
риски заключены в ***приемлемые рамки*** *и остаются таковыми.*

Управлять рисками нужно на всем жизненном цикле ИС

Анализ

- Известные риски – учитываем при выработке требований (как к системе в целом, так и к средствам безопасности)

Разработка

- Изучение рисков помогает выбрать соответствующие решения, в том числе архитектурные (ключевые для безопасности)

Установка

- Выявленные риски учитывают при конфигурировании, тестировании и проверке требований

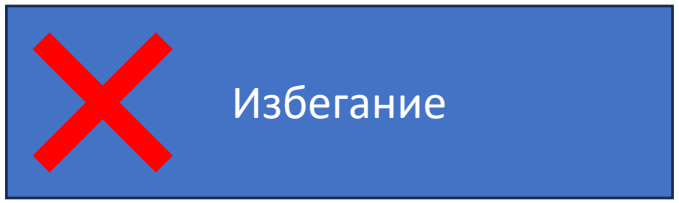
Эксплуатация

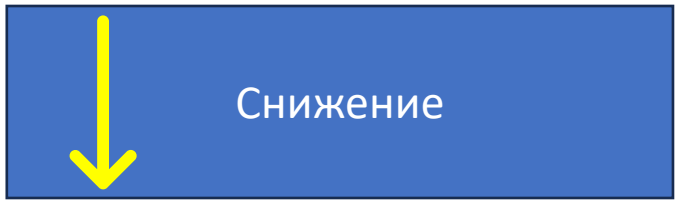
- Сопровождение всех существенных изменений в системе

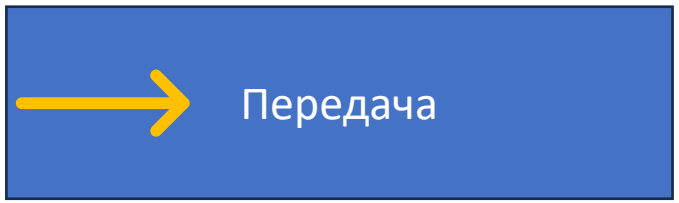
Вывод из эксплуатации

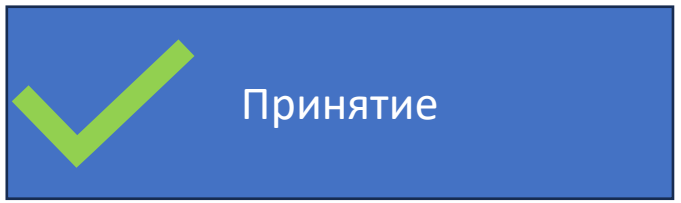
- Убедиться в том, что данные (информация, которая защищается) не разглашаются и остаются в нужном статусе

Управление рисками

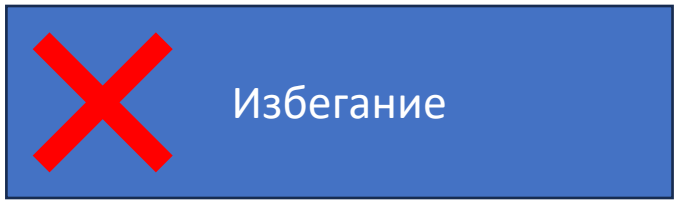








Метод управления рисками: избегание риска



- Принятие мер ДО того, как риск совершится
- Постоянное совершенствование активов для своевременного выявления уязвимостей
- Не применять ПО, которое не известно с точки зрения уязвимостей (слишком новое)
- Не применять ПО, в котором слишком много уязвимостей (слишком старое)
- Иногда, лучше отказаться от каких-либо новых проектов, чтобы НЕ рисковать

Метод управления рисками: передача риска

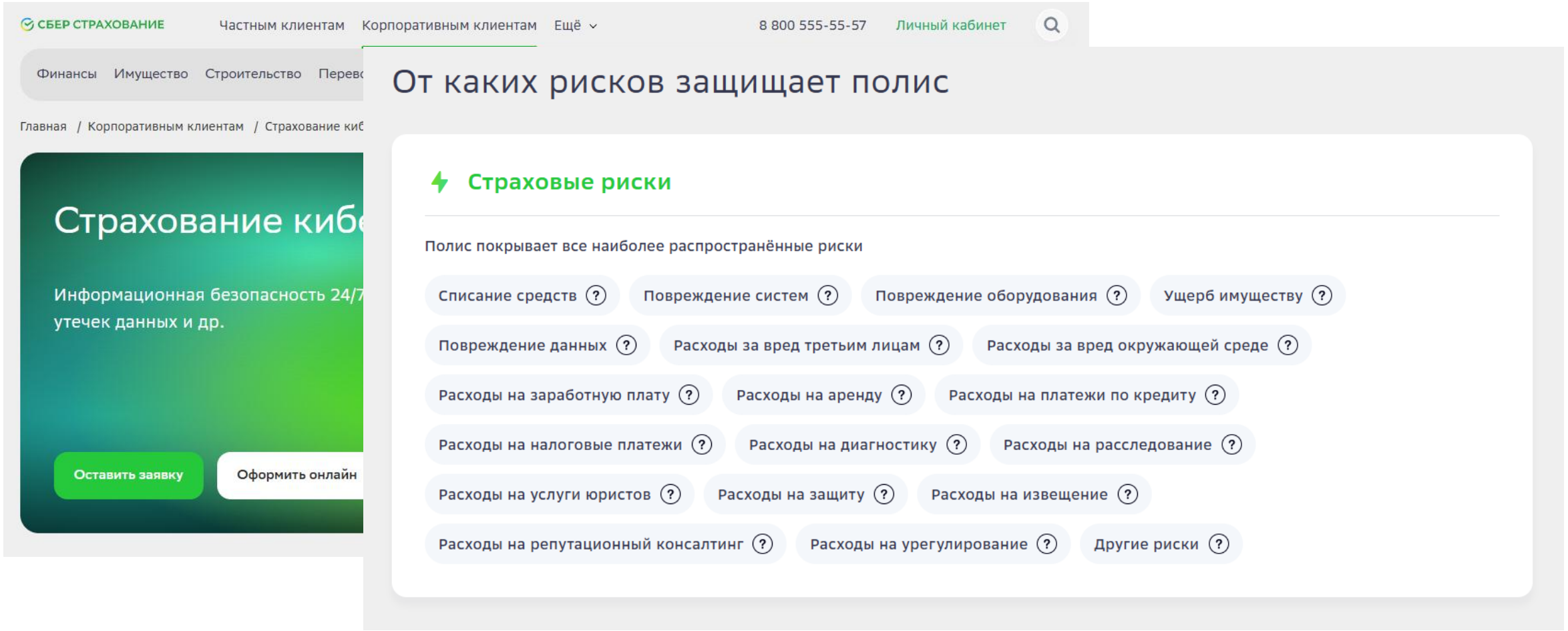
Передача

Передача финансовой ответственности другим лицам (страховым компаниям)

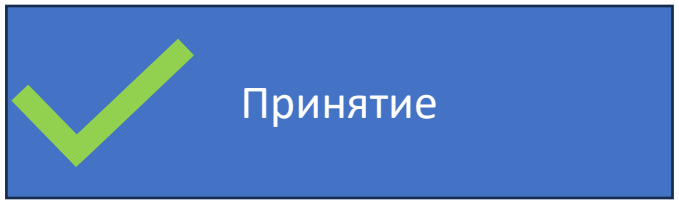
Заключение соглашений об уровне сервиса (SLA) для ответственности поставщиков/подрядчиков

Получение части сервисов кибербезопасности от других компаний (SOC, защита от DDoS-атак, защита электронной почты, антивирус и пр.)

Метод управления рисками: передача риска



Метод управления рисками: принятие риска



Определение уровня риска, ниже которого риски будут рассматриваться как «допустимые».

Отслеживание «примлемых» рисков продолжается, о них нельзя забывать, т.к. значение риска может выйти за пределы

Используется для «балансировки» фокуса организации на высокие риски

Метод управления рисками: снижение риска

Снижение

Снижение вероятности реализации уязвимости

$$R = P_{\text{угрозы}} \times P_{\text{уязвимости}} \times D$$

Снижение вероятности угроз

Снижение цены потери (наносимого ущерба)

Снижение риска: вероятность угрозы

Как снизить вероятность угрозы?

Повлиять на «источник» угрозы

Усложнить реализацию угрозы (повысить «ставки» и сложность реализации)

Повышение грамотности сотрудников (чтобы не выполняли действий)

Применить защитные меры и/или средства защиты

Снижение риска: вероятность реализации уязвимости

Как снизить вероятность реализации уязвимости?

Обновиться на «новую» версию

Применить меры, рекомендуемые разработчиком ПО/АО

Применить защитные меры и/или средства защиты

Снижение риска: вероятность реализации уязвимости

Как снизить вероятность реализации уязвимости?

При разработке ПО применять анализ с помощью специализированных инструментов

Статический анализ приложений (SAST): анализ исходного кода

Динамический анализ приложений (DAST): проверка во время выполнения

Интерактивный анализ приложений (IAST): комбинация SAST и DAST

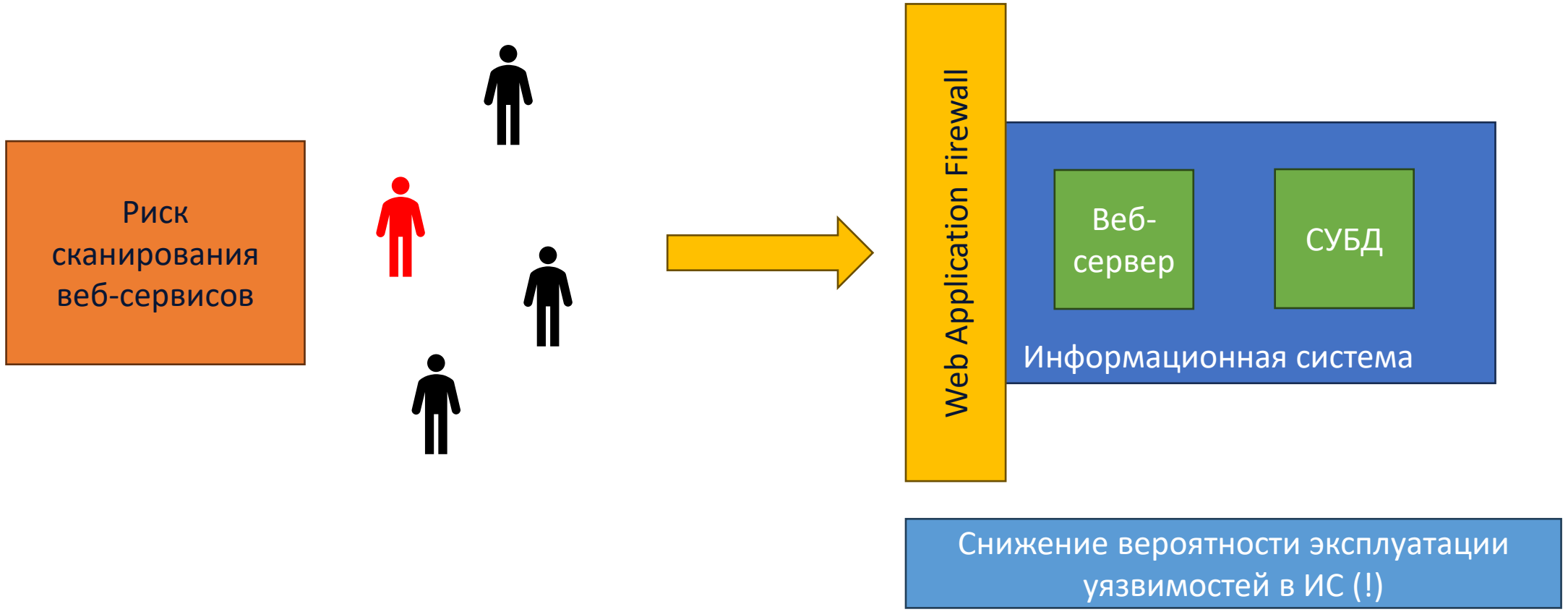
Анализ мобильных приложений (MAST)

Снижение риска: снижение цены потери (ущерба)

Как снизить цену потери (ущерба)?

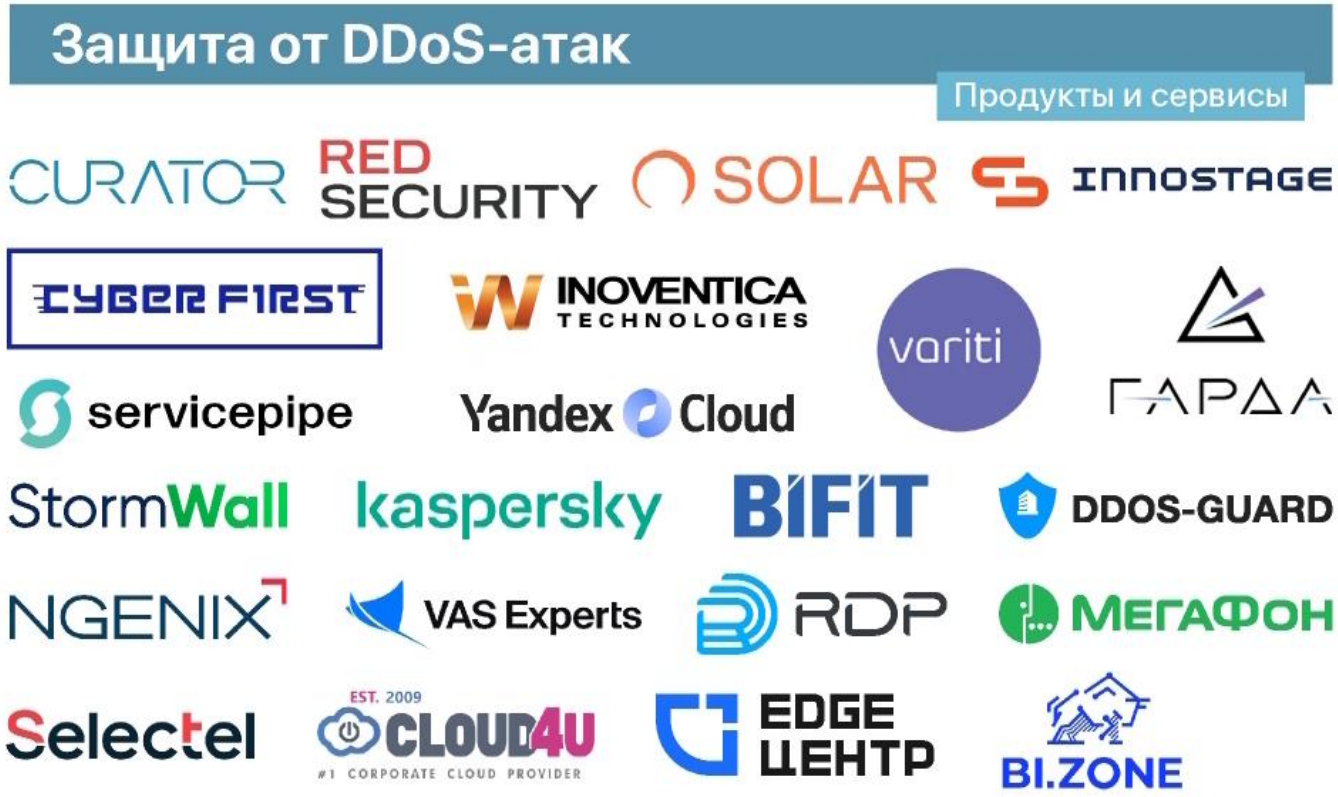
- Корректно оценивать потенциальный ущерб
- Применять архитектуру ИС так, чтобы ущерб не относился ко всей системе, а только к части
- Сокращать время «простоя» по причине реализации риска

Снижение рисков за счет применение средств защиты



Средства защиты информации: защита веб-приложений

Средства защиты информации: защита от DDoS-атак



Средства защиты информации: межсетевые экраны и IPS/IDS

Средства защиты информации: антивирусы и защита ПК

Средства защиты информации: виртуальные частные сети

Средства защиты информации: учетные записи и доступ

Средства защиты информации: привилегированный доступ

Контроль действий привилегированных пользователей (PAM)

Контур, ИНДИД, NGRSOFTLAB, BI.ZONE, AVSOFT, КОМПАНИЯ АКТИВ, AVANPOST, НОВЫЕ ТЕХНОЛОГИИ БЕЗОПАСНОСТИ, webcontrol, АЙТИБАСТИОН, INNOSTAGE, SOLAR

Средства защиты информации: криптография

Что будет на семинаре № 7?

- Готовые самостоятельные работы высылаем лектору

- Защита самостоятельных работ перед семинаристами:
  - Демонстрация презентаций (по командам)
  - Защита каждым студентом своей части (1-го слайда с рисками)


ВЫСШАЯ • ШКОЛА • ЭКОНОМИКИ •