Программная инженерия

Москва
2026

Лекция № 6.
Оценка рисков

Основы кибербезопасности

Белявский Д.А.


Риски

Что такое риск?

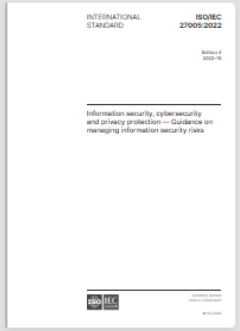
потенциальная проблема

вероятные потери в результате инцидентов

комбинация вероятности события и его последствий

предполагаемое событие, способное принести кому-либо ущерб или убыток

Определение риска



ISO/IEC 27005:2022

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

Published (Edition 4, 2022)

Риск информационной безопасности – потенциальная возможность использования **уязвимостей** актива или группы активов конкретной **угрозой** для причинения **ущерба** организации.

Пример из лекции №2: Может ли автомобиль быть в безопасности?

Кража

Природные явления

Угон

Пожар

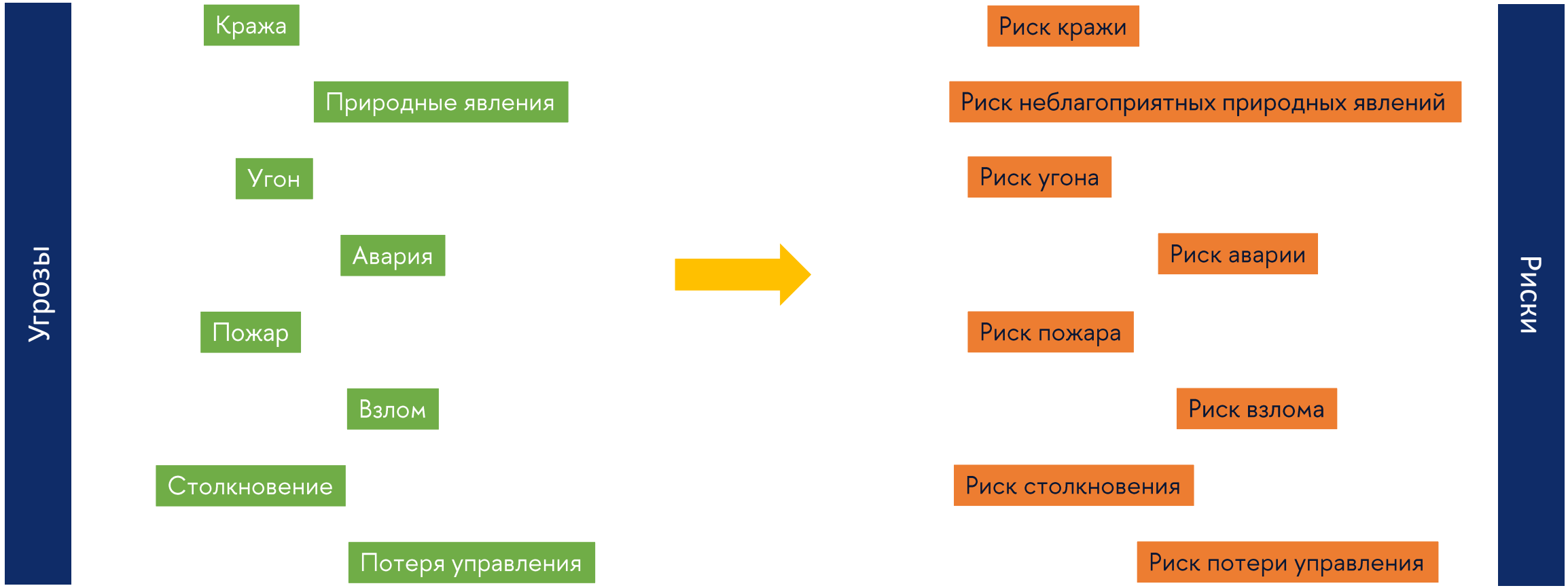
Авария

Столкновение

Потеря управления

Взлом

Переведем в риски



Как сравнить риски между собой?

Риски	Вероятность события		Ущерб (цена потери)		Значение
Риск кражи (например, колеса)	2%	×	100 000 ₽	=	2 000 ₽
Риск неблагоприятных природных явлений	5%		50 000 ₽		2 500 ₽
Риск угона	0,1%		1 000 000 ₽		1 000 ₽
Риск аварии	8%		200 000 ₽		16 000 ₽
Риск пожара	0,05%		1 000 000 ₽		500 ₽
Риск взлома	0,1%		50 000 ₽		50 ₽
Риск столкновения	15%		100 000 ₽		15 000 ₽
Риск потери управления	3%		500 000 ₽		15 000 ₽

52 050 ₽

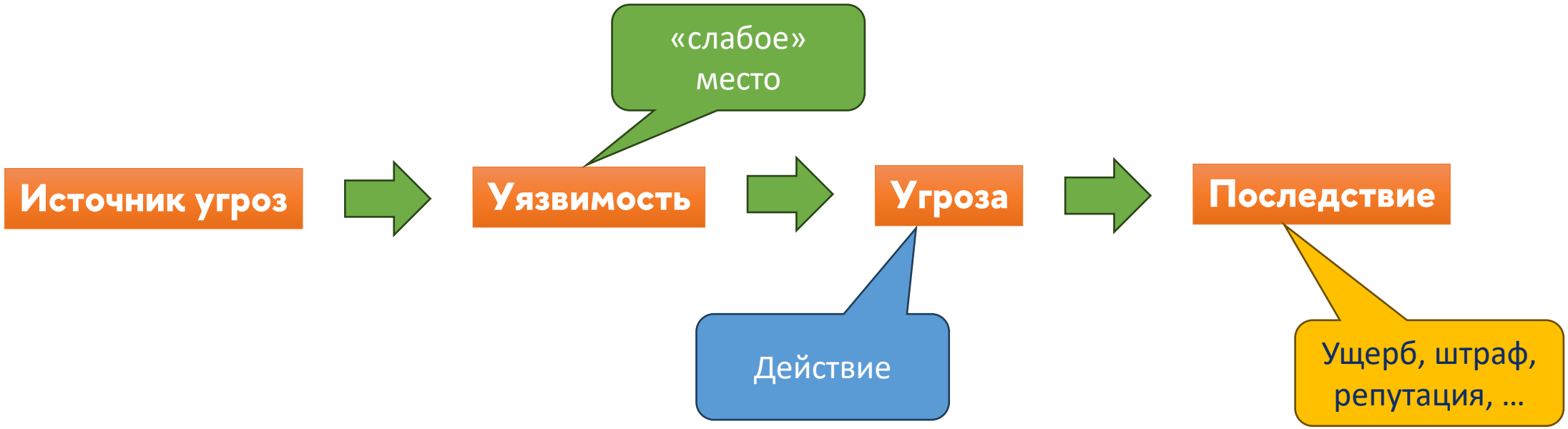
Стоимость автомобиля: 1 млн ₽

Вернемся в кибербезопасность

- Риск кражи данных
- Риск утечки информации
- Риск неблагоприятных природных явлений
- Риск аварии в системе
- Риск пожара
- Риск кибератаки
- Риск взлома
- Риск потери управления
- Риск заражения вирусом (вредоносным ПО)
- Риск сбоя ПО (баги)
- Риск недоступности системы от DDoS-атак
- Риск подбора пароля
- Риск расшифрования хранимых данных
- Риск фишинга

И другие...

Взаимосвязь источников, уязвимостей и угроз



От чего зависит риск?

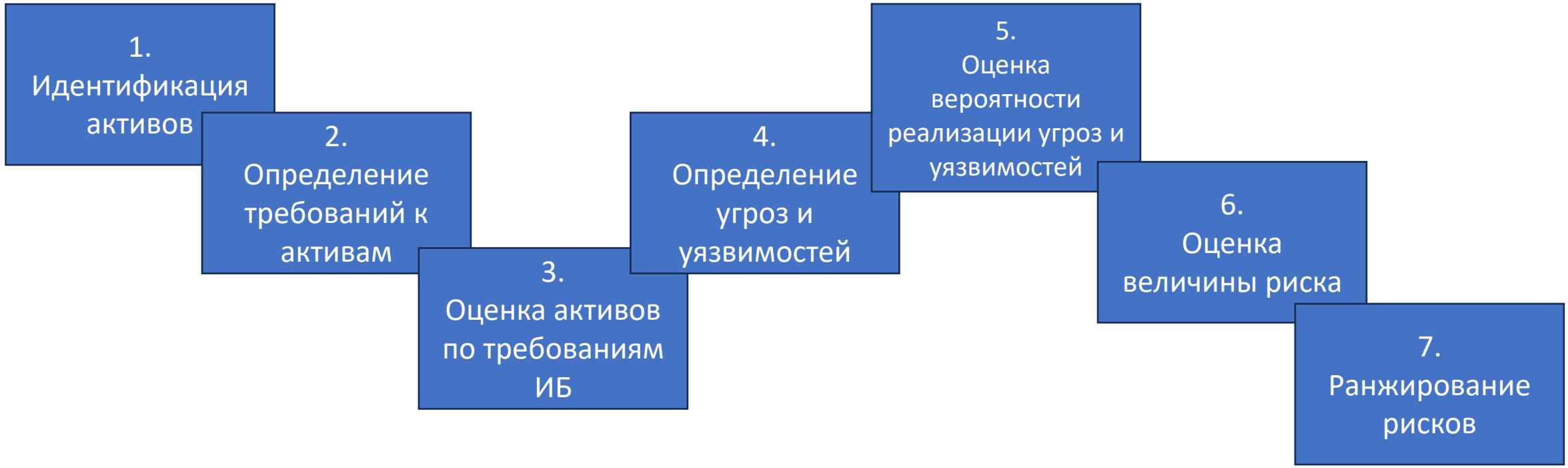
Уязвимость **Угроза** **Последствие**

Риск, как комплексный показатель, учитывается, когда все факторы риска (угроза, уязвимость и последствие/ущерб) рассматриваются вместе.

Зачем нужно знать и учитывать риски?

Разработка мер	Создание методов учета	Допустимый риск
Меры, позволяющие снизить риск или избежать нежелательного риска	Методы учета рисков при принятии решений (бизнес-решений)	Определение уровней допустимого (приемлемого риска) и насколько можем «рисковать»

Процесс анализа рисков



Качественная оценка рисков

Вероятность реализации риска

	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Очень низкое	0	1	2	3	4
Низкое	1	2	3	4	5
Среднее	2	3	4	5	6
Высокое	3	4	5	6	7
Очень высокое	4	5	6	7	8

Влияние на бизнес организации

Шкала выбирается произвольно, но применяется для ВСЕХ рисков при их оценке

Количественная оценка рисков

$$R = P_{\text{событие}} \times D$$

R – риск

D – ущерб

Цена потери

$P_{\text{событие}}$ – вероятность

$$P_{\text{событие}} = P_{\text{угрозы}} \times P_{\text{уязвимости}}$$

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


Информационная система

Информационная система

Информационная система – система, которая предназначается для хранения, обработки, поиска и/или передачи информации (данных), и включает в себя соответствующие информационные активы и организационные ресурсы (человеческие, финансовые и т.д.).

ИС - это комплекс

ИС ≠ Программное обеспечение

Активы в ИТ (и в кибербезопасности)

Цифровые активы

Активы ПО

Исполняемое ПО

Исходный код

Неисполняемое ПО
(конфигурации, словари и др.)

Виртуальное ИТ-оборудование

Цифровые информационные активы
(контент, например, документы, аудио-, видео-, графика, базы данных и др.)

ИТ-оборудование

Физическое ИТ-оборудование
(серверы, устройства, оборудование связи и др.)

Физический носитель
(содержащий цифровые активы, включая резервные копии)

Лицензии на ИТ-активы

Контракты (договора) по ИТ-активам

Система управления ИТ-активами
(хранит информацию об активах, метаданые)

Сервисы ИТ-активов
(комбинация ИТ-активов, внешних, например, SaaS, техническое обслуживание и пр.)

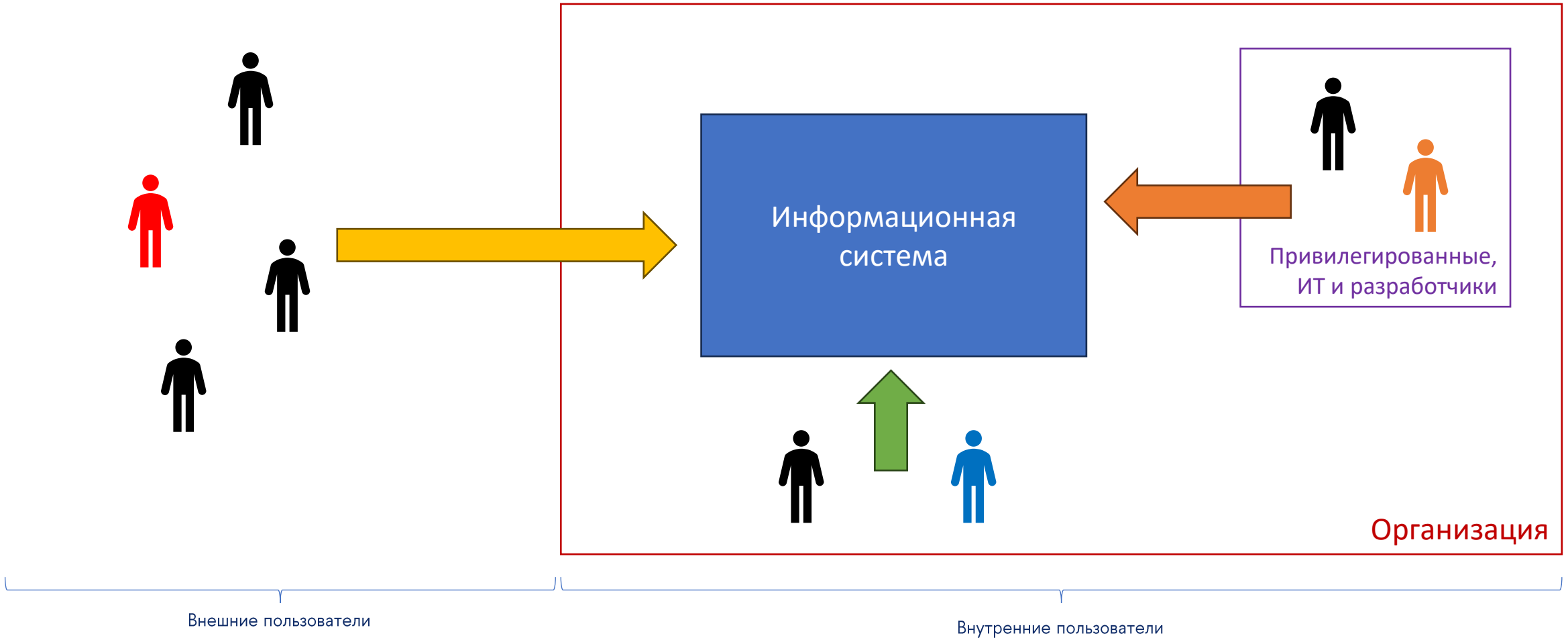
Не ИТ-активы
(персонал, необходимый для использования ИТ-активов)

Стандарт
ГОСТ Р ИСО/МЭК 19770-1-2021

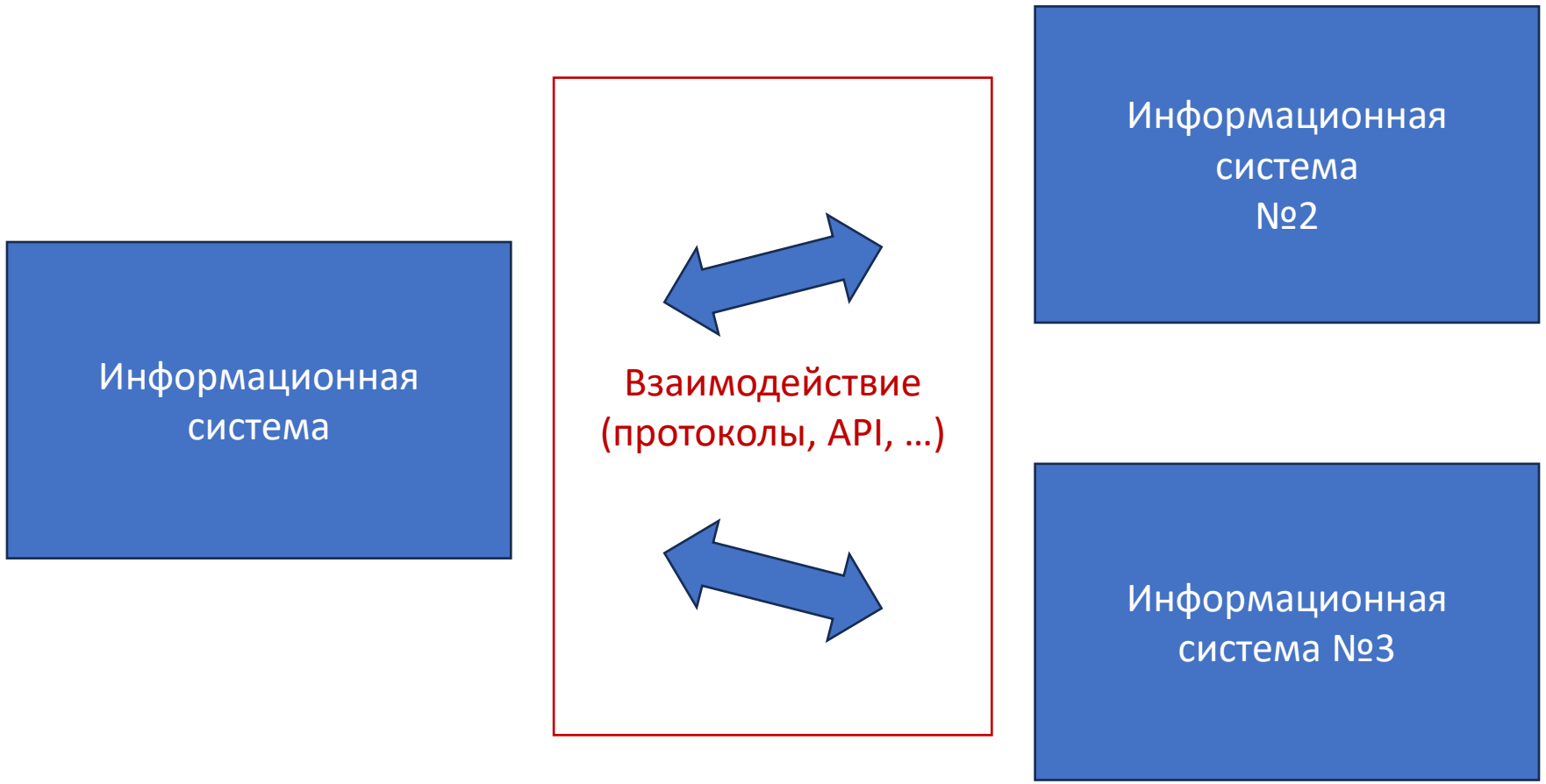
ИС: Оборудование (аппаратное обеспечение)

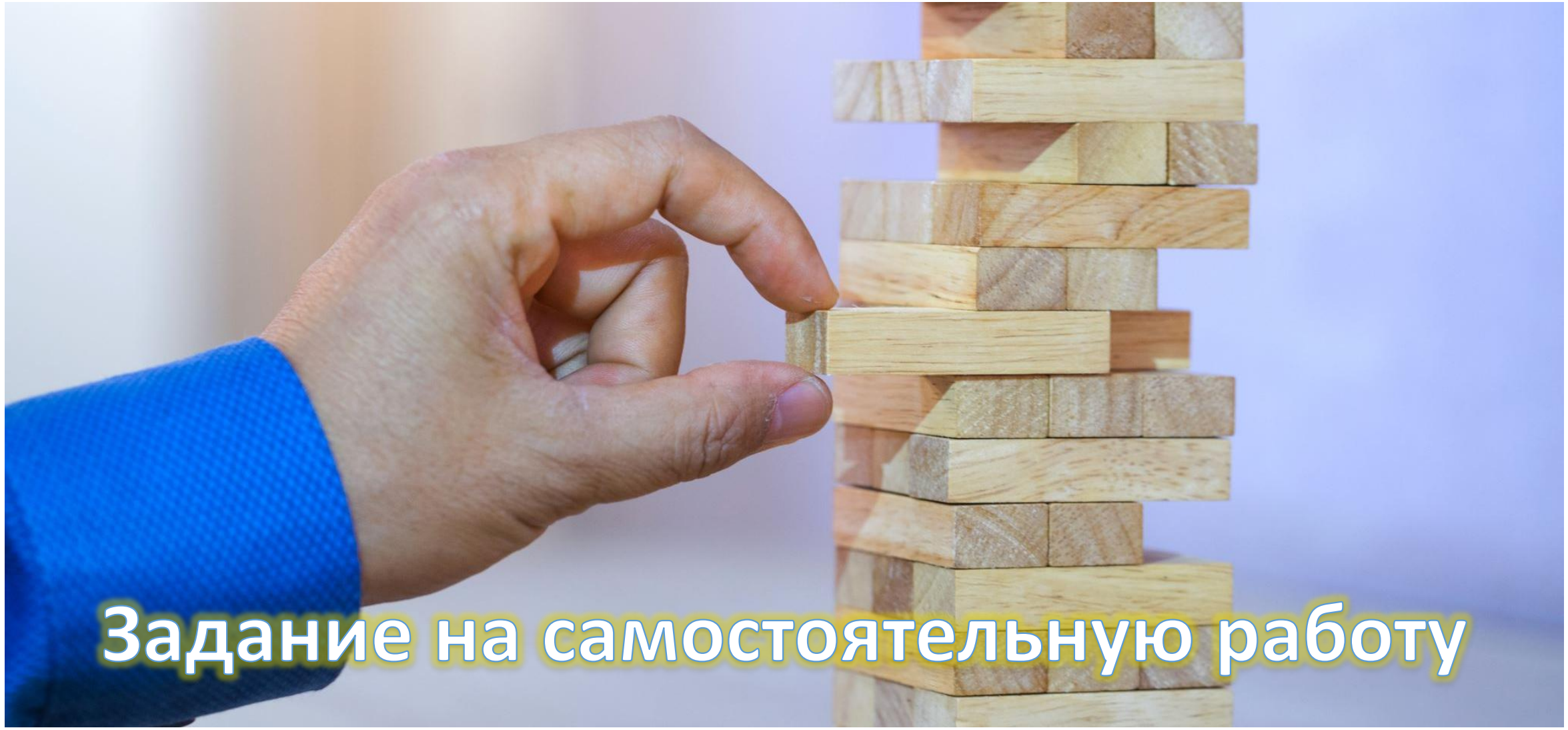
ИС: программное обеспечение

ИС: Пользователи



ИС: Взаимодействие систем




Задание на самостоятельную работу

Выбор организации

2 команды НЕ выбрали организацию

- 4 энергоблок
- Чемпионы

Ведомость с результатами контрольных работ.
И список организаций по КОМАНДАМ

2 команды выбрали ОДИНАКОВУЮ организацию

- Cherrypickme
- Тимур и его команда

Шаг 1. Информационная система

Шаг 1.
Определить Информационную систему в Организации

Это НЕ программное обеспечение

Это комплекс, нацеленный на выполнение какой-либо задачи

Обычно, применяется для автоматизации каких-либо бизнес-процессов

Рассчитать стоимость ИС.
Как сумма всех закупок по конкретной ИС.

Шаг 1. Информационная система
Примеры информационных систем

Государственная информационная система «Региональный электронный бюджет Московской области»

Информационная система «Единый центр управления регионом»

Информационная система «Сквозной учет назначения и проведения высокотехнологичной медицинской помощи»

Автоматизированная информационная система ОМС «Персонифицированный учет оказанной медицинской помощи»

Номер «закупки» (или тендера) - некорректно

Ссылка на «закупку» - некорректно

Программное обеспечение - некорректно

Техническая поддержка - некорректно

Шаг 2. Определить состав ИС – программное обеспечение

В рамках данной самостоятельной работы рассматриваем ТОЛЬКО программное обеспечение, как состав ИС

Автоматизированная информационная система ОМС «Персонифицированный учет оказанной медицинской помощи»

ОС для серверов приложений – IBM AIX 7.2

СУБД Oracle Database 11g

Среда разработки (фреймворк)
Java (версия не ниже 1.8)

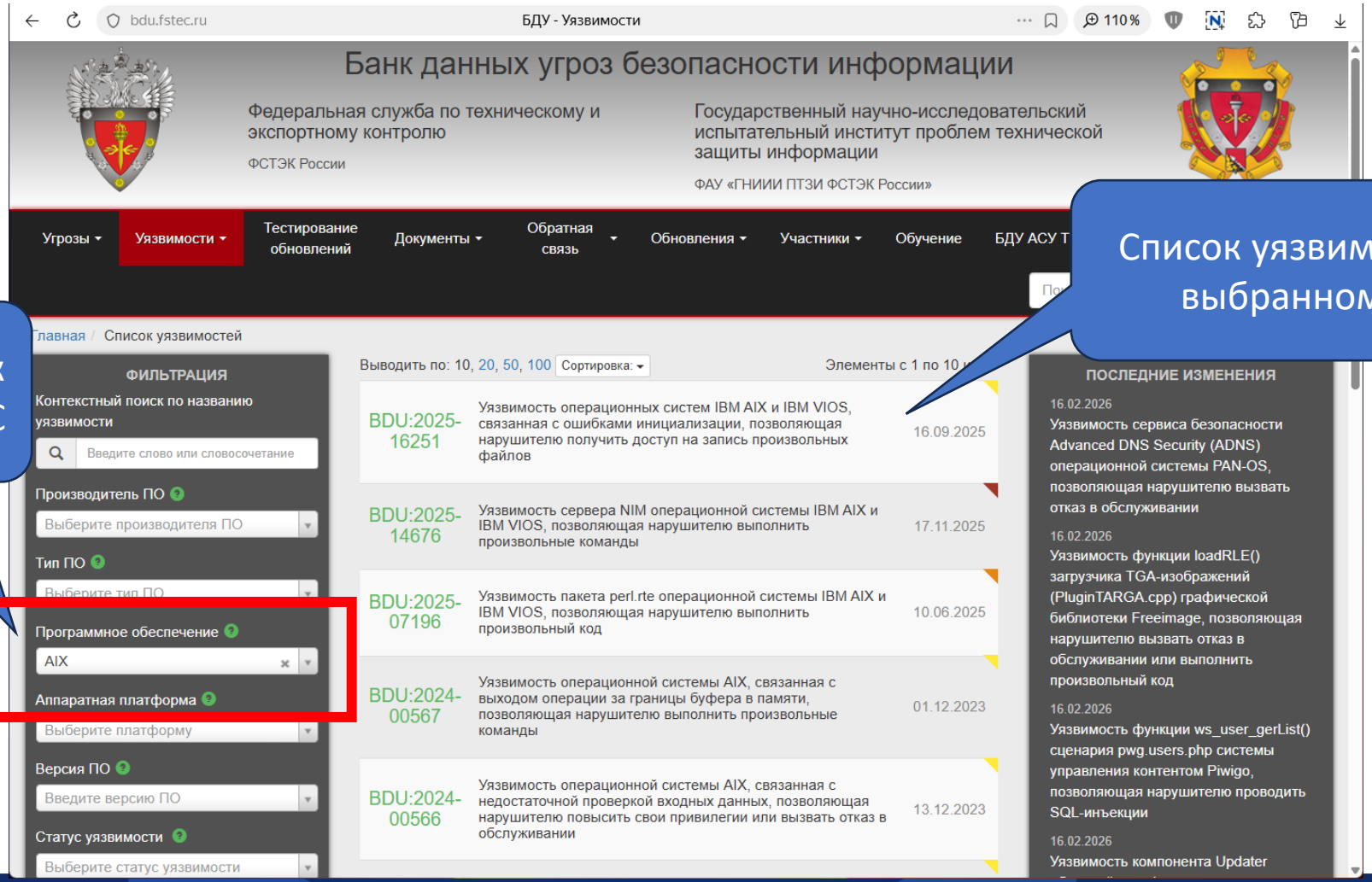
Шаг 3. Исследовать уязвимости в ПО

cve.mitre.org

bdu.fstec.ru

vulners.com

Шаг 3. Исследовать уязвимости в ПО



Производим поиск по ПО в составе ИС

Список уязвимостей по выбранному ПО

Шаг 3. Исследовать уязвимости в ПО

Записываем НОМЕР уязвимости и ее описание

Проверяем, относится ли выбранная уязвимость к ПО из состава ИС

Сверяем ВЕРСИИ программного обеспечения с собранными из документации

BDU:2025-16251 Вид

Описание уязвимости: Уязвимость операционных систем IBM AIX и IBM VIOS связана с ошибками инициализации. Эксплуатация уязвимости может позволить нарушителю получить доступ на запись произвольных файлов

Уязвимое ПО

Вендор	Наименование ПО	Версия ПО	Тип ПО	Архитектура (Платформа)
IBM Corp.	AIX	7.2	Операционная система	Не указана
IBM Corp.	IBM Vios	3.1	Операционная система	Не указана
IBM Corp.	AIX	7.3	Операционная система	Не указана
IBM Corp.	IBM Vios	4.1	Операционная система	Не указана

Операционные системы и аппаратные платформы:
IBM Corp. AIX 7.2
IBM Corp. IBM Vios 3.1
IBM Corp. AIX 7.3
IBM Corp. IBM Vios 4.1

Тип ошибки: Внешняя инициализация надежных переменных или массивов данных (CWE-454)

Класс уязвимости: Уязвимость кода

Дата выявления: 16.09.2025

Базовый вектор уязвимости:
CVSS 2.0: AV:L/AC:H/Au:N/C:C/I:C/A:C
CVSS 3.0: AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS 4.0: Вектор не задан

Уровень опасности уязвимости:
Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6,2)
Высокий уровень опасности (базовая оценка CVSS 3.1 составляет 7,4)

Шаг 3. Исследовать уязвимости в ПО

BDU:2025-16251 Вид

Описание уязвимости	Уязвимость операционных систем IBM AIX и IBM VIOS связана с ошибками инициализации. Эксплуатация уязвимости может позволить нарушителю получить доступ на запись произвольных файлов

Уязвимое ПО

Вендор	Наименование ПО	Версия ПО	Тип ПО	Архитектура (Платформа)
IBM Corp.	AIX	7.2	Операционная система	Не указана
IBM Corp.	IBM Vios	3.1	Операционная система	Не указана
IBM Corp.	AIX	7.3	Операционная система	Не указана
IBM Corp.	IBM Vios	4.1	Операционная система	Не указана

Операционные системы и аппаратные платформы	IBM Corp. AIX 7.2 IBM Corp. IBM Vios 3.1 IBM Corp. AIX 7.3 IBM Corp. IBM Vios 4.1
Тип ошибки	Внешняя инициализация надежных переменных или массивов данных (CWE-4
Класс уязвимости	Уязвимость кода
Дата выявления	16.09.2025
Базовый вектор уязвимости	CVSS 2.0: AV:L/AC:H/Au:N/C:C/I:C/A:C CVSS 3.0: AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H CVSS 4.0: Вектор не задан
Уровень опасности уязвимости	Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6,2) Высокий уровень опасности (базовая оценка CVSS 3.1 составляет 7,4)

Записываем «уровень опасности уязвимости»

Шаг 3. Исследовать уязвимости в ПО

ПО из состава ИС	Уязвимость (номер и описание)	Уровень опасности уязвимости	$P_{уязвимости}$
IBM AIX 7.1 и выше	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	Средний уровень опасности (базовая оценка CVSS 2.0 составляет 6,2) Высокий уровень опасности (базовая оценка CVSS 3.1 составляет 7,4)	= 7,4 / 10 = 74%
IBM AIX 7.1 и выше	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	Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10) Критический уровень опасности (базовая оценка CVSS 3.1 составляет 10)	= 10 / 10 = 100%

Есть несколько алгоритмов расчета опасности – CVSS 2.0, CVSS 3.1 и др.

Выберите ОДИН алгоритм и используйте для ВСЕХ выявленных уязвимостей

Например, выбираем CVSS 3.1

Шаг 4. Связываем уязвимости с угрозами

Банк данных угроз безопасности информации

https://bdu.fstec.ru

ФСТЭК России

Шаг 4. Связываем уязвимости с угроз

Предполагаем, на основе источника угрозы

Уязвимость (номер и описание)	$P_{\text{уязвимости}}$	Угроза, с помощью которой может быть реализована уязвимость	$P_{\text{угрозы}}$
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%	УБИ.015 Угроза доступа к защищаемым файлам с использованием обходного пути **Источник угрозы:** Внешний нарушитель с низким потенциалом; Внутренний нарушитель с низким потенциалом	75%
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%	УБИ.195 Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы **Источник угрозы:** Внешний нарушитель с высоким потенциалом	25%

Шаг 5. Оцениваем риски

Цена потери (ущерб) расцениваем как СТОИМОСТЬ всей информационной системы

Риск	Угроза, с помощью которой может быть реализована уязвимость	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;	BDU:2025-16251 Уязвимость операционных систем IBM AIX и IBM VIOS связана с ошибками инициализации. Эксплуатация уязвимости может позволить нарушителю получить доступ на запись	= 7,4 / 10 = 74%	75%	15 401 522,33	8 547 844,89
Риск удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	вредоносного кода в обход механизмов защиты операционной системы **Источник угрозы:** Внешний нарушитель с высоким потенциалом	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

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

Шаг 6. Ранжируем риски

Риск	Угроза, с помощью которой может быть реализована уязвимость	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	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		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	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

Сортировка по значению рассчитанного риска
От большего к меньшему

Шаг 7. Ваши варианты минимизации рисков

Что нужно сделать в организации, чтобы снизить значение рисков?

Какой уровень рисков для организации может быть приемлемым?

Какие действия должны предпринять разработчики ИС, чтобы снизить риски?

Что будет на семинаре № 6?

- Готовим вопросы по выполнению самостоятельной работы
- Тест по теме «оценка рисков»


ВЫСШАЯ • ШКОЛА • ЭКОНОМИКИ •