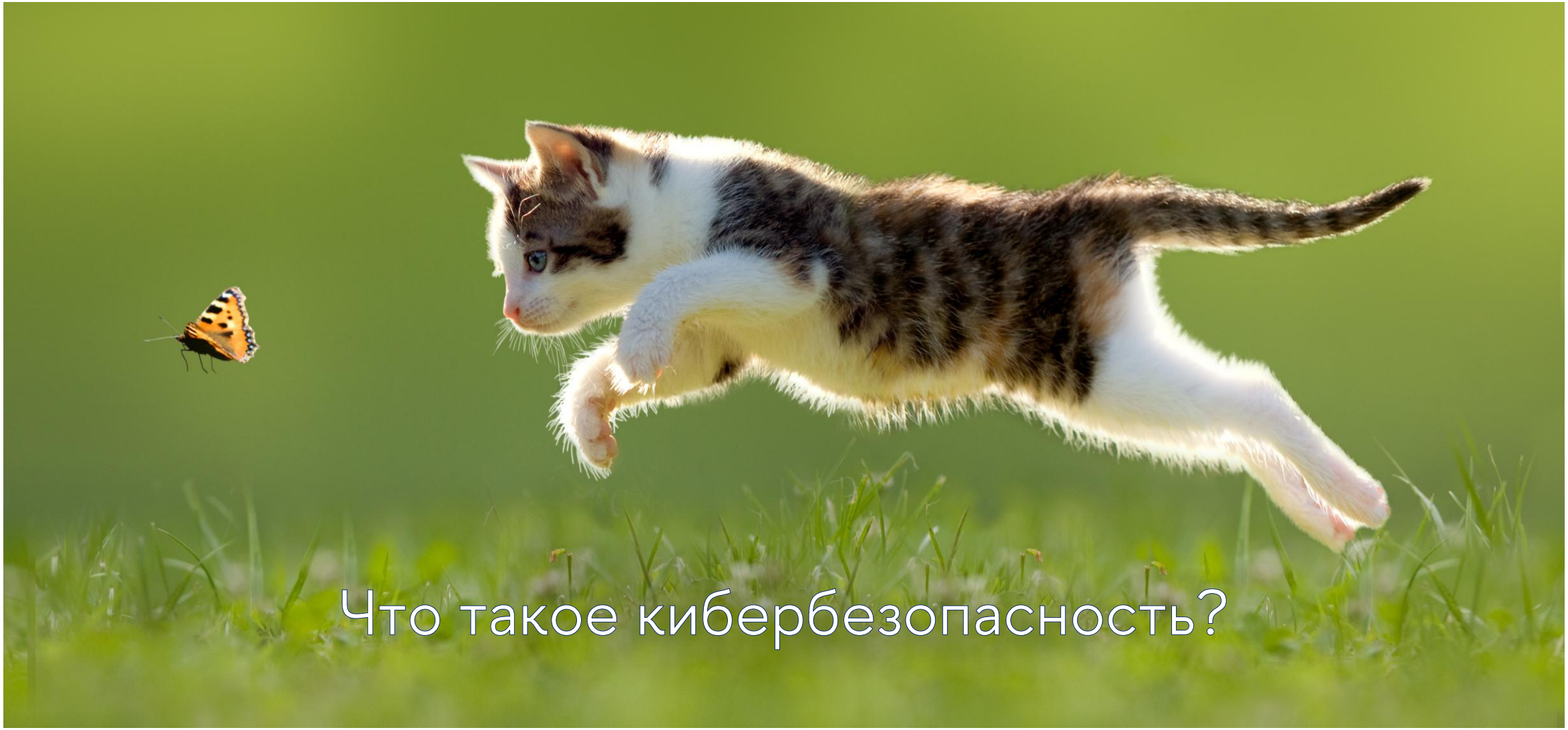
Программная инженерия

Москва
2026

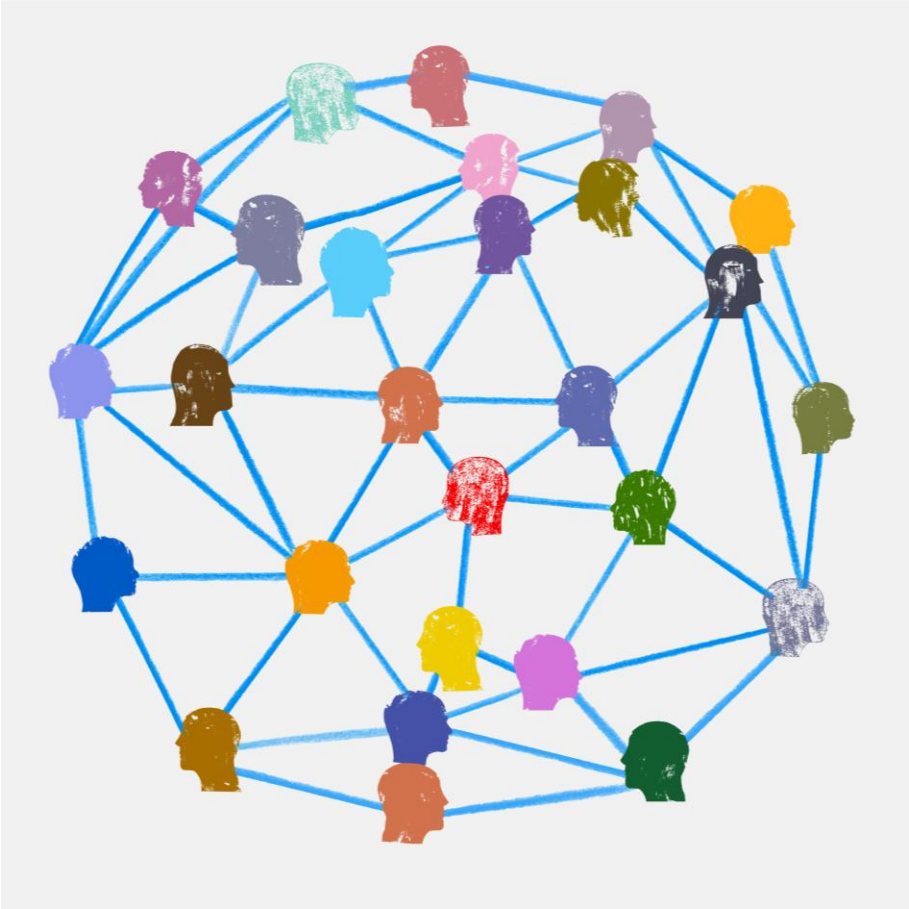
Лекция № 1. Задача обеспечения информационной безопасности

Основы кибербезопасности

Белявский Д.А.



Что такое кибербезопасность?



Кибербезопасность – это целый мир со своими правилами и стандартами

Хобби

Покупки

Новости

Путешествия

Общение

Личность

Государство

Развлечения

Транспорт

Бизнес

Игры

Знания

Исследования


Если этого ничего не будет?

Что будете делать?

Конечно, будете защищать!

Учетная запись → dbelyavskiy@hse.ru

Пароль → Pass1234

Не верьте ;)

Как выбрать пароль?

Какой пароль достаточно безопасный?

Как правильно хранить пароли?

Как в системах хранятся пароли пользователей?

Достаточно ли безопасносно использовать пароль из 4-х цифр?

А из 4-х символов (буквы, цифры, пунктуация)?

Рекомендуется выбирать пароль не менее 8 символов
(+добавим русские буквы)

Достаточно ли безопасносно использовать пароль из 4-х цифр?

$10 \times 10 \times 10 \times 10 = 10^4 \Rightarrow$ 10 000 вариантов

А из 4-х символов (буквы, цифры, пунктуация)?

$94^4 \Rightarrow$ 78 074 896 вариантов

Рекомендуется выбирать пароль не менее 8 символов
(+добавим русские буквы)

$160^8 \Rightarrow$ 429 496 729 600 000 000 вариантов

Сколько у вас учетных записей?

Как вы храните пароли?

Как рекомендуется хранить пароли?

Что можем использовать вместе или вместо пароля?

Face ID

Двух-факторная аутентификация

Много-факторная аутентификация

Одноразовый код

PUSH-код

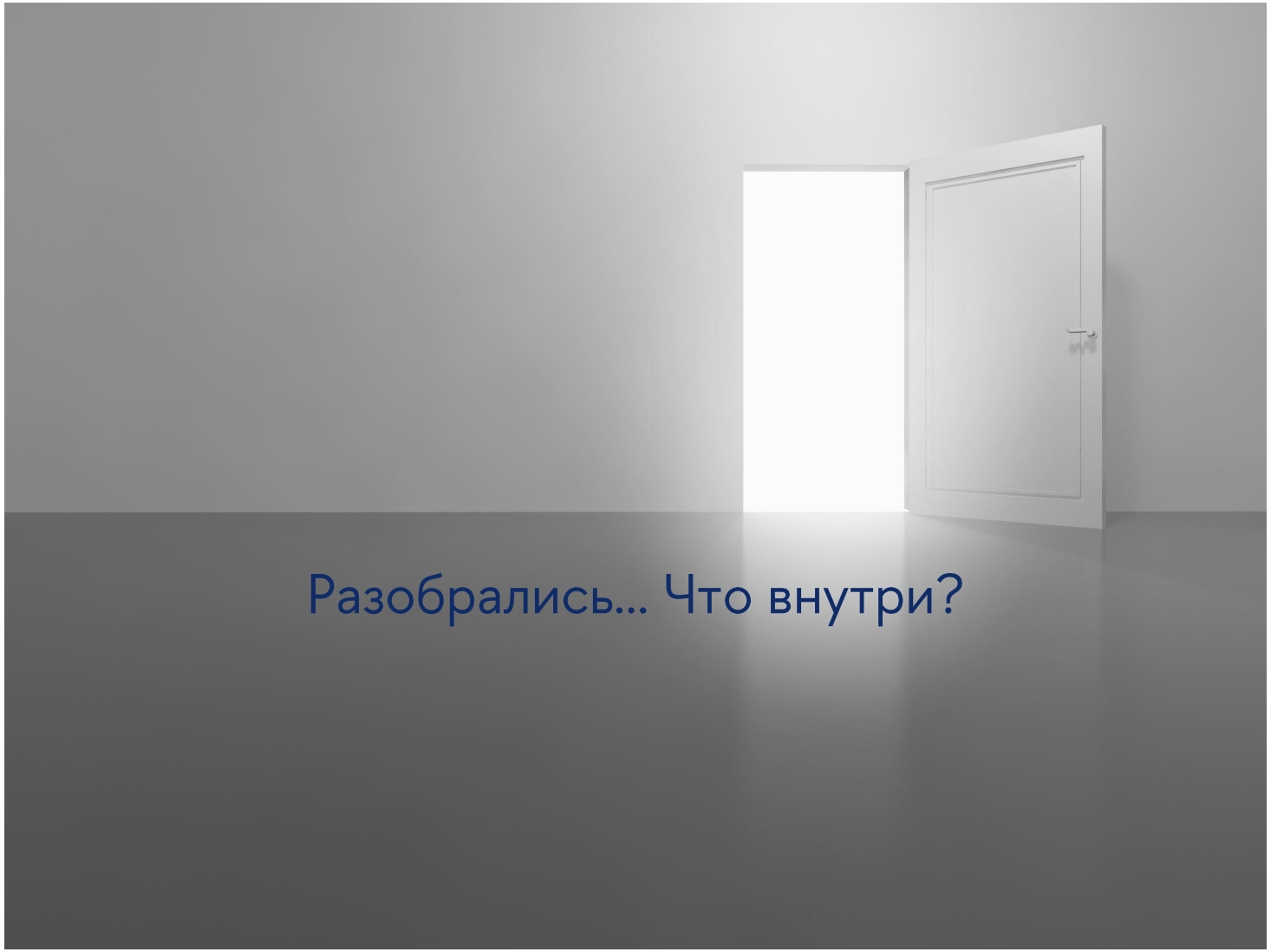
PIN-код

Аутентификация через стороннюю систему (OAuth)

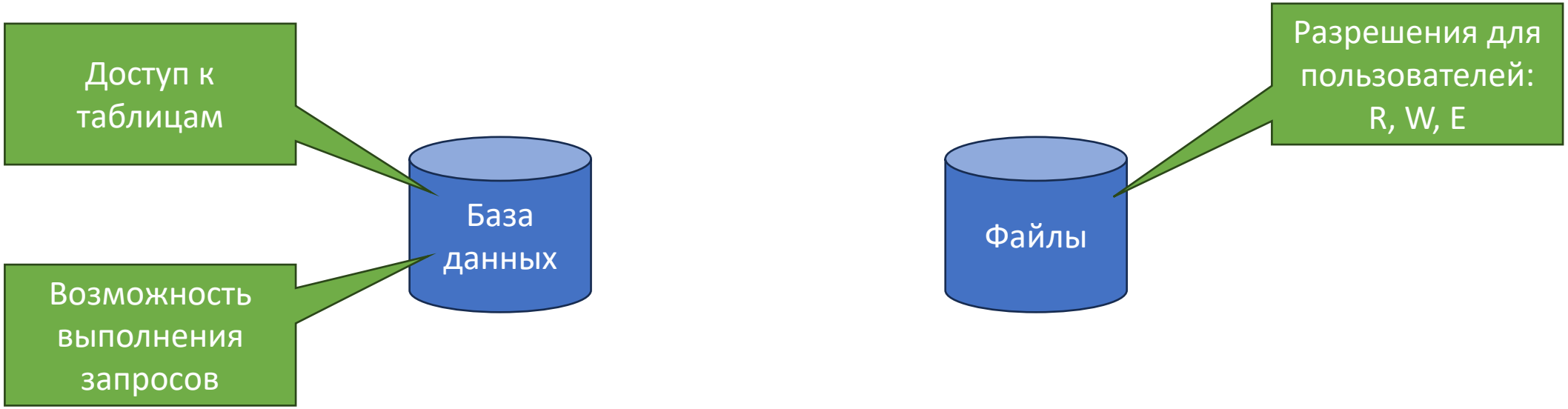
SMS-код

Биометрия

Отпечаток пальца


Разобрались... Что внутри?

Мы вошли в какую-либо систему. Как мы получим доступ к информации?



Информация хранится в открытом виде?

ДА

Например:
- Системные идентификаторы
- Имена учетных записей (пользователей)
- Номер телефона
- ...

НЕТ, или НЕ рекомендуется

Например:
- Пароли
- Ключи доступа к серверам/устройствам
- Токены доступа к API
- ...

Способ сокрытия данных от посторонних

Шифрование

Расшифрование

Кодирование

Хэширование

Задача обеспечения информационной безопасности

От кого защищаем информацию?

Злоумышленники

Вот тут «хакеры»

Могут быть и свои сотрудники

Ошибки

Ошибки в коде, в конфигурации

Природа

Град, шторм, наводнение…

Повреждение

Испортили

Технические сбои

Любая техника рано или поздно сломается

Информационная безопасность:

Конфиденциальность — Информация доступна только для авторизованных лиц

Целостность — Неизменность информации и ее достоверность

Доступность — Авторизованные лица могут иметь доступ без ограничений

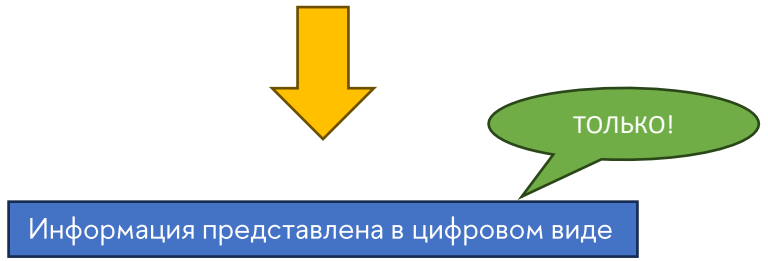
Информационная безопасность

или

Кибербезопасность

Защита информации: физическая, нормативная, компьютерная

Цель: правильное управление обработкой информации



Защита информации: компьютерная

Цель: создание и применение средств защиты информации

Для всего в кибербезопасности есть правила (лучшие практики), стандарты, требования законодательства и отдельных организаций

HTTPS

Bug Bounty

ЭЦП

PenTest

TLS

152-ФЗ

CVE

ФСБ

AES

TOTP

SHA-2

КоАП

RSA

ISO 27000

УК

NIST 800-50

PCI DSS

DevSecOps

ФСТЭК

Что будет на семинаре № 1?

- Знакомство с преподавателями,
  которые будут проводить семинары
- Вводный тест,
  чтобы оценить ваши знания до начала дисциплины
  (без оценивания)
- Вопросы по курсу и смежным тематикам
  (мы собираем, чтобы рассказать вам что-то интересеное или что-то подробнее)


ВЫСШАЯ • ШКОЛА • ЭКОНОМИКИ •