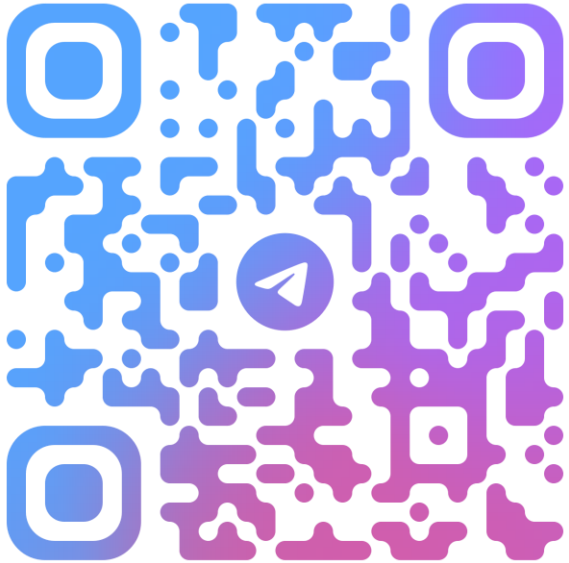
Программная инженерия

Москва
2026

Лекция № 2.
Угрозы и нарушители

Основы кибербезопасности
Белявский Д.А.

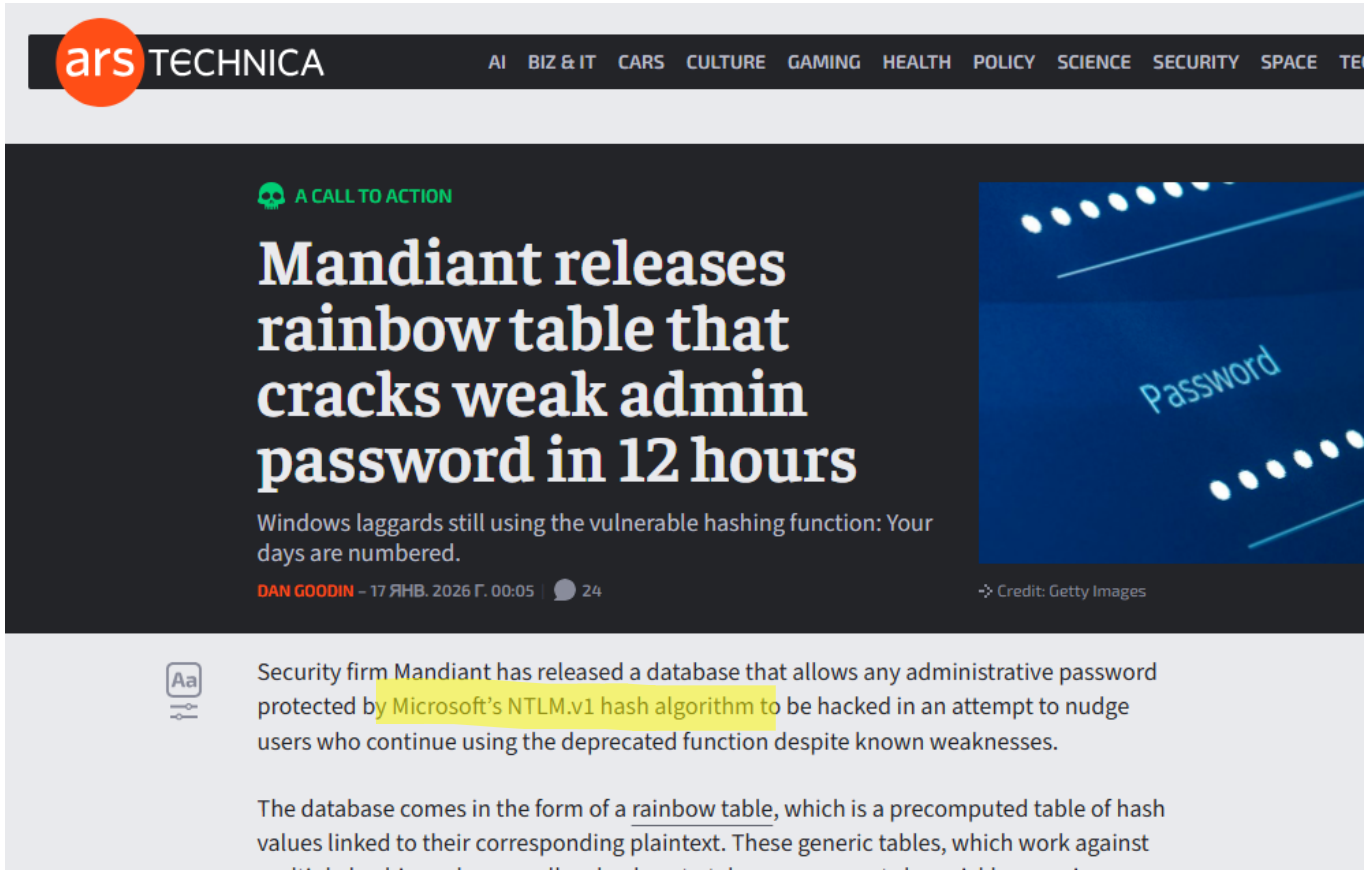
Общение – группа в Телеграме



Взлом пароля в 8 символов возможен за 12 часов

Mandiant Cybersecurity Consulting

17.01.2026



ars TECHNICA

AI BIZ & IT CARS CULTURE GAMING HEALTH POLICY SCIENCE SECURITY SPACE TE

A CALL TO ACTION

Mandiant releases rainbow table that cracks weak admin password in 12 hours

Windows laggards still using the vulnerable hashing function: Your days are numbered.

DAN GOODIN – 17 ЯНВ. 2026 Г. 00:05 | 24

Credit: Getty Images

Security firm Mandiant has released a database that allows any administrative password protected by Microsoft's NTLM.v1 hash algorithm to be hacked in an attempt to nudge users who continue using the deprecated function despite known weaknesses.

The database comes in the form of a rainbow table, which is a precomputed table of hash values linked to their corresponding plaintext. These generic tables, which work against

https://arstechnica.com/security/2026/01/mandiant-releases-rainbow-table-that-cracks-weak-admin-password-in-12-hours/


Безопасность

Безопасность

Состояние, а не процесс.

Вы защищены?

Или, вы в безопасности?

Пример: Может ли автомобиль быть в безопасности?

Кража

Природные явления

Угон

Пожар

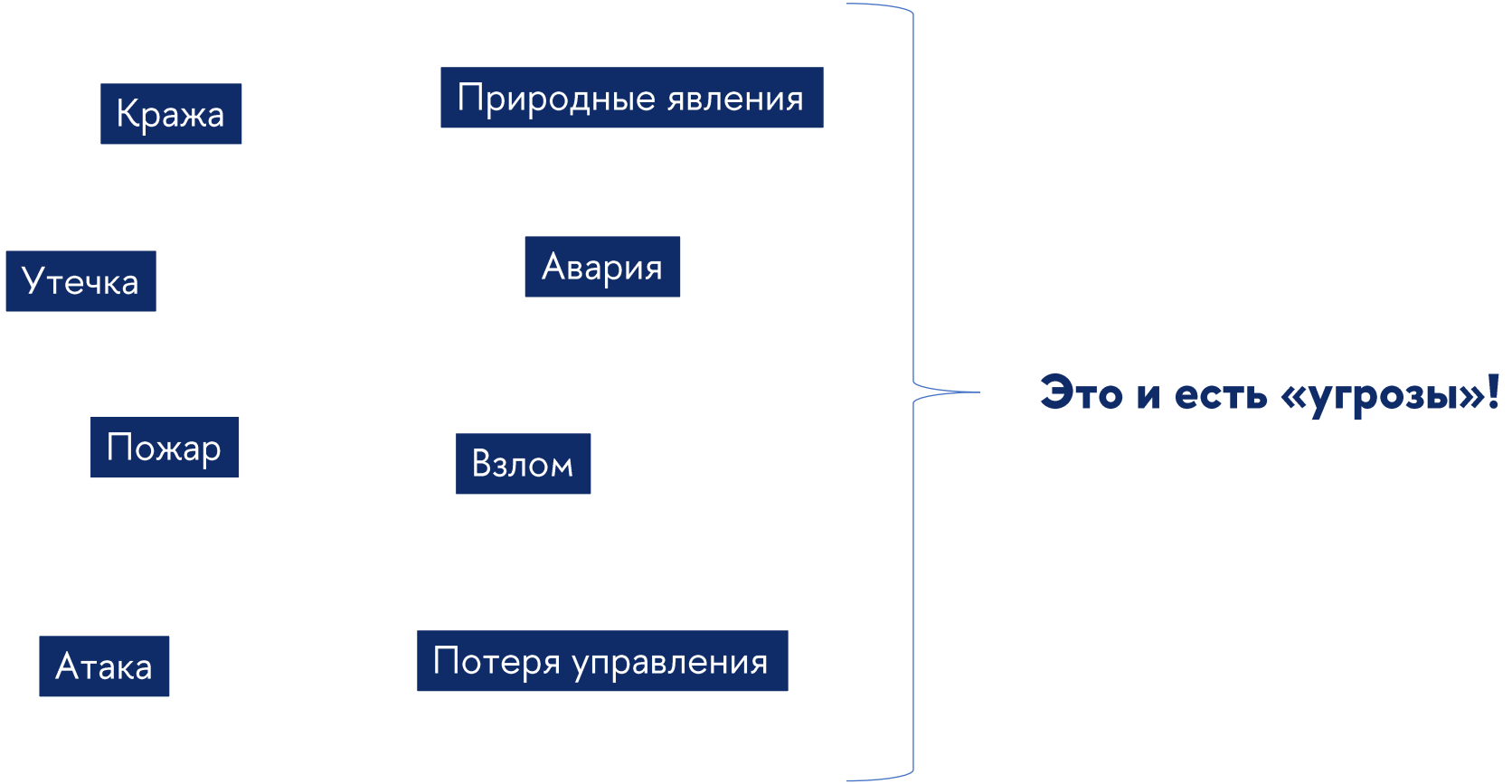
Авария

Столкновение

Потеря управления

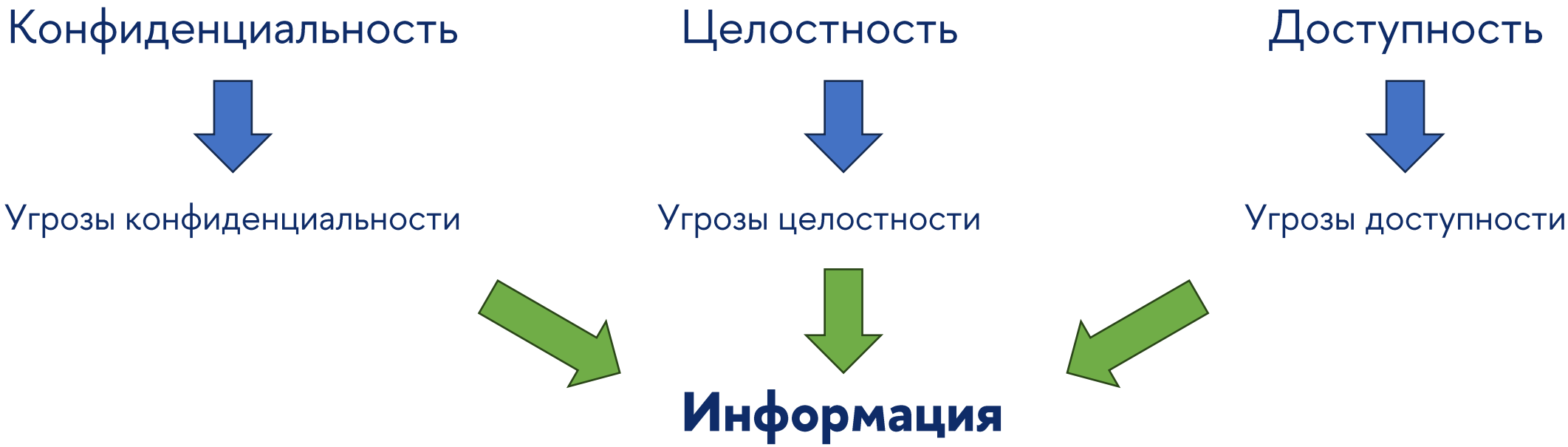
Взлом

Информация подверждена схожим «неприятностям»



Угрозы безопасности информации

Угроза – потенциальная возможность определенным образом нарушить информационную безопасность



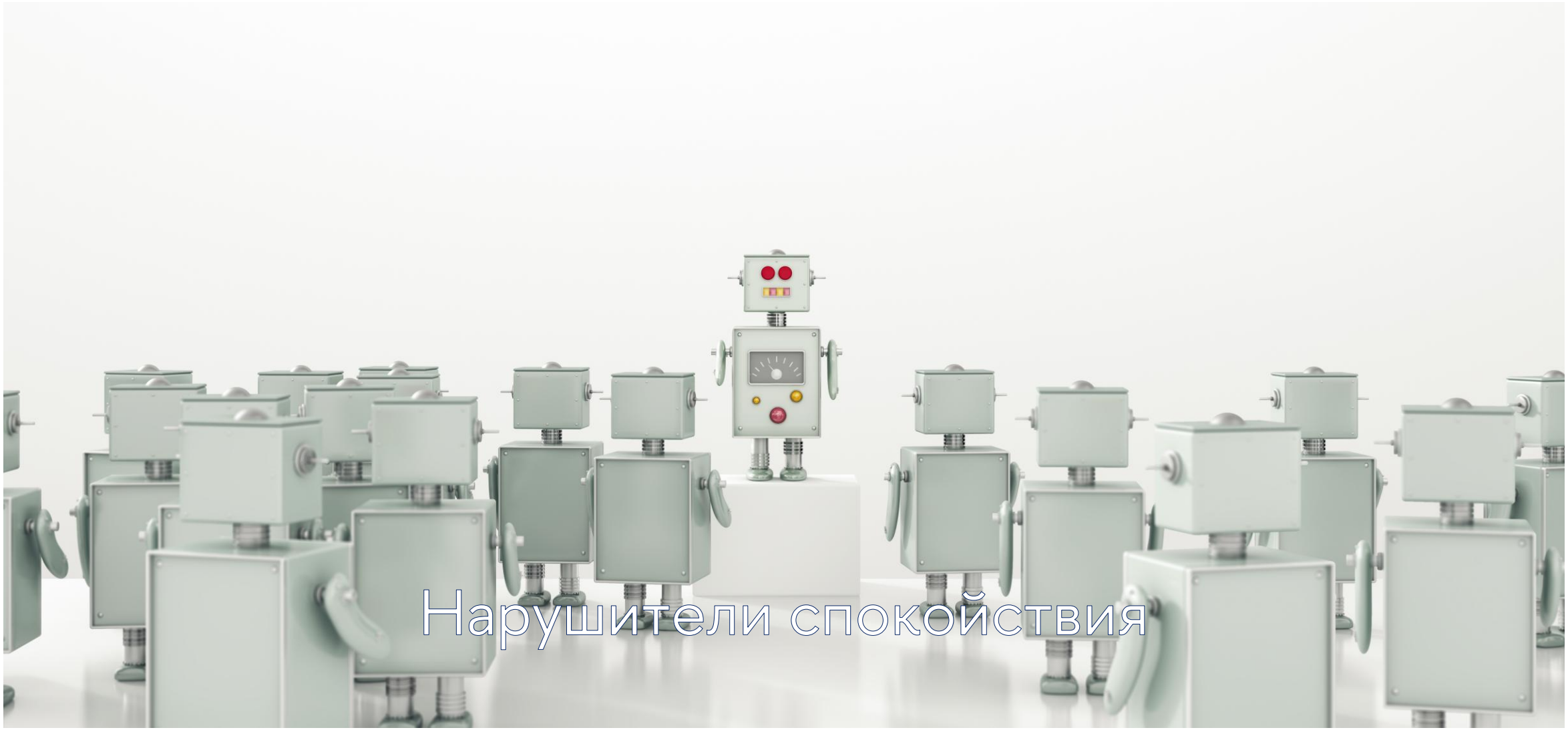
Каталог угроз безопасности

ФСТЭК России

Федеральная служба по техническому
и экспортному контролю

Банк данных угроз безопасности информации

https://bdu.fstec.ru


Нарушители спокойствия

Источники угроз

Источники угроз

Субъекты

Объекты

Источник угроз – исходные причины потенциального воздействия на безопасность информации

Группы источников угроз

Антропогенные

Техногенные

Стихийные

Классификация источников угроз

- Международные
- Политические
- Национальные
- Экономические
- Военные
- ...

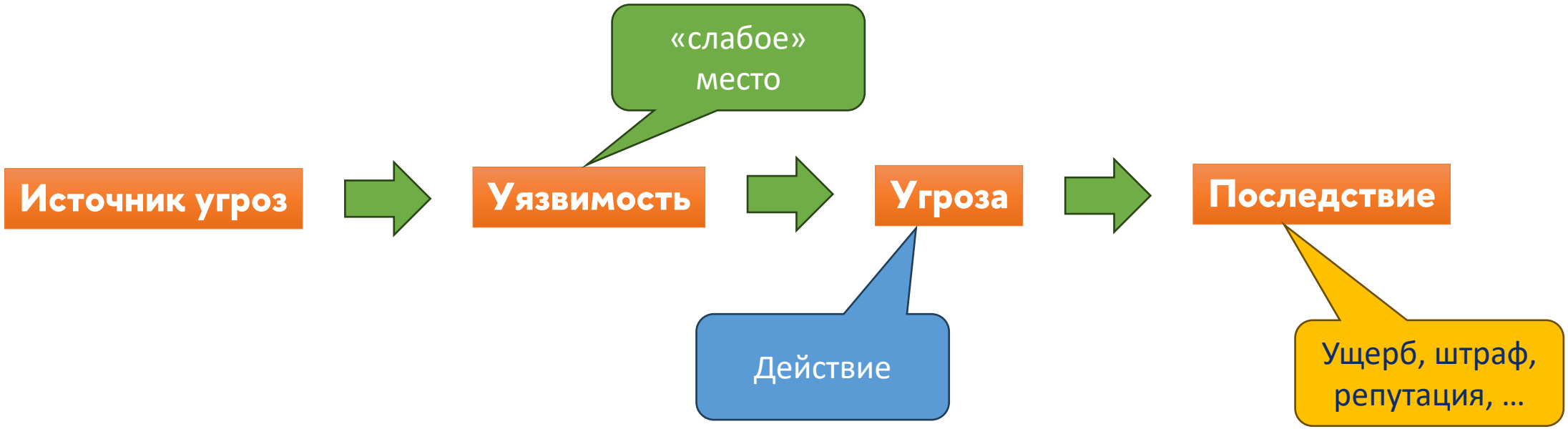
- Недостаточность развития нормативной законодательной базы
- Снижение качества образования
- Некачественные ИТ-товары
- Некачественные услуги

Внешние источники

- недостаток финансирования
- отсутствие внимания на ИБ
- технологическое отставание (или отрыв)
- недостаточная квалификация

Внутренние источники

Взаимосвязь источников, уязвимостей и угроз



Уязвимость

Уязвимость – причина, приводящая (или которая может привести) к нарушению безопасности информации

Уязвимости обусловлены

- свойствами архитектуры информационной системы (программы)
- используемыми протоколами обмена и интерфейсами
- недостатками в процессах функционирования объекта информационной системы
- применяемым программным обеспечением
- применяемым аппаратным обеспечением
- невнимательностью сотрудников (некомпетентностью)
- условиями эксплуатации

Каталоги уязвимостей ПО (и частично устройств)

cve.mitre.org

bdu.fstec.ru

VULNERS COM

Кто может воспользоваться уязвимостями и реализовать угрозу?

Кто может быть нарушителем?

Зачем нужно знать нарушителя?

Конечно же, для того, чтобы предугадать возможные действия!

Моделируем!

Кто может действовать?

Какие мотивы (цели)?

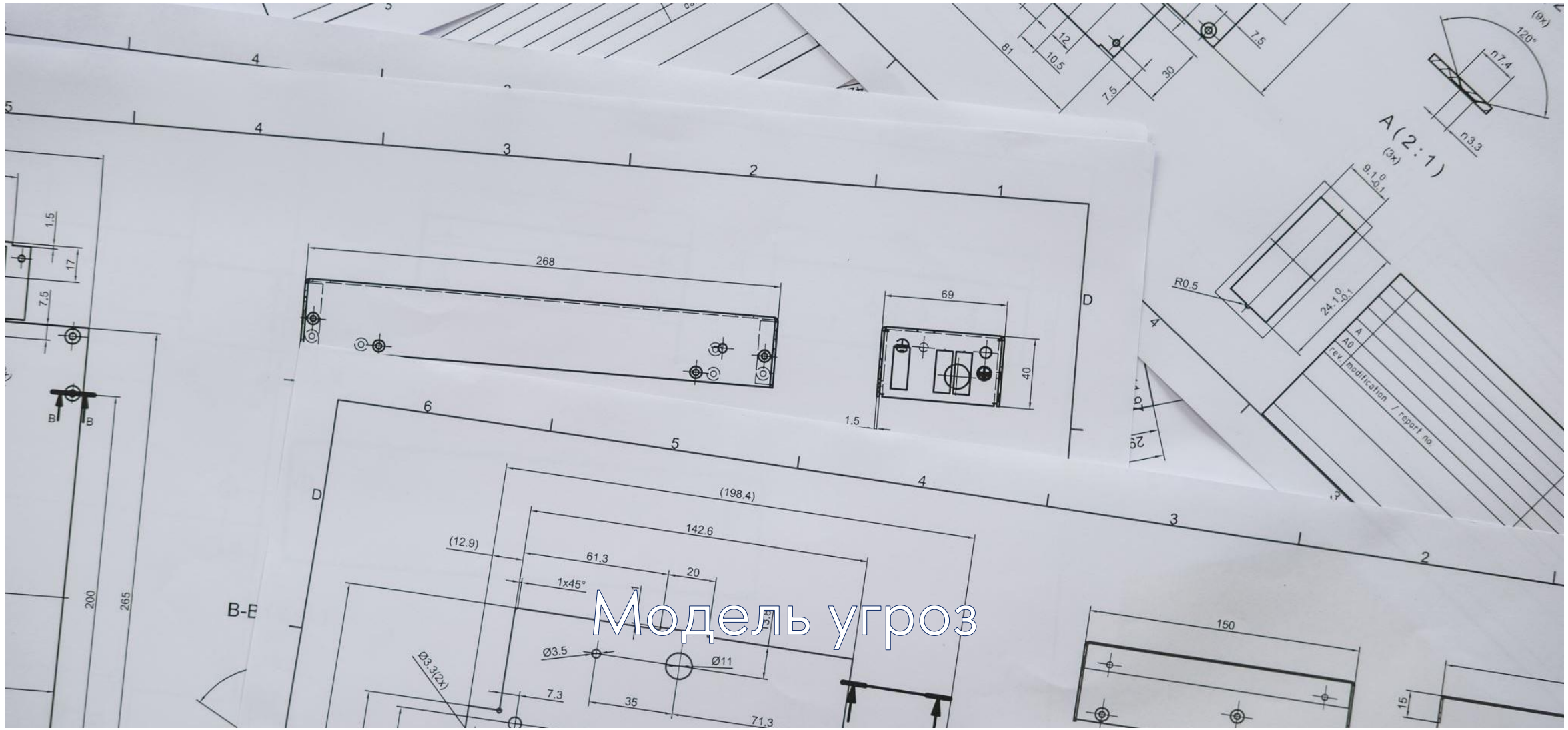
Какая квалификация?

Какое техническое оснащение?

Какие ограничения?

Какой характер действий?

Основные мотивы нарушителей: Безответственность | Самоутверждение | Корыстный интерес



Модель угроз

Модель угроз

Модель угроз – систематизированный перечень актуальных угроз безопасности информации при их обработке в информационной системе

1. Это документ!

2. Основа для планирования и осуществления мероприятий по безопасности

3. Для обоснованных требований по безопасности к разрабатываемым или уже эксплуатируемым информационным системам

4. В неё включаются:
- модель нарушителя
- актуальные угрозы
- меры по минимизации/нейтрализации угроз и последствий
- применение средств защиты информации

Что будет на семинаре № 2?

- Обсуждение по прошедшим темам лекций
- Обсуждение результатов вводного теста
- Контрольная работа по терминам (БУДЬТЕ ГОТОВЫ!!)


ВЫСШАЯ • ШКОЛА • ЭКОНОМИКИ •