

Форум для специалистов по информационной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВУЗа: ПРОБЛЕМЫ, УГРОЗЫ, ПУТИ РЕШЕНИЯ
(КиберВолга – 2025) CyberVolga – 2025

📍 Онлайн платформа Virtual Mirapolis

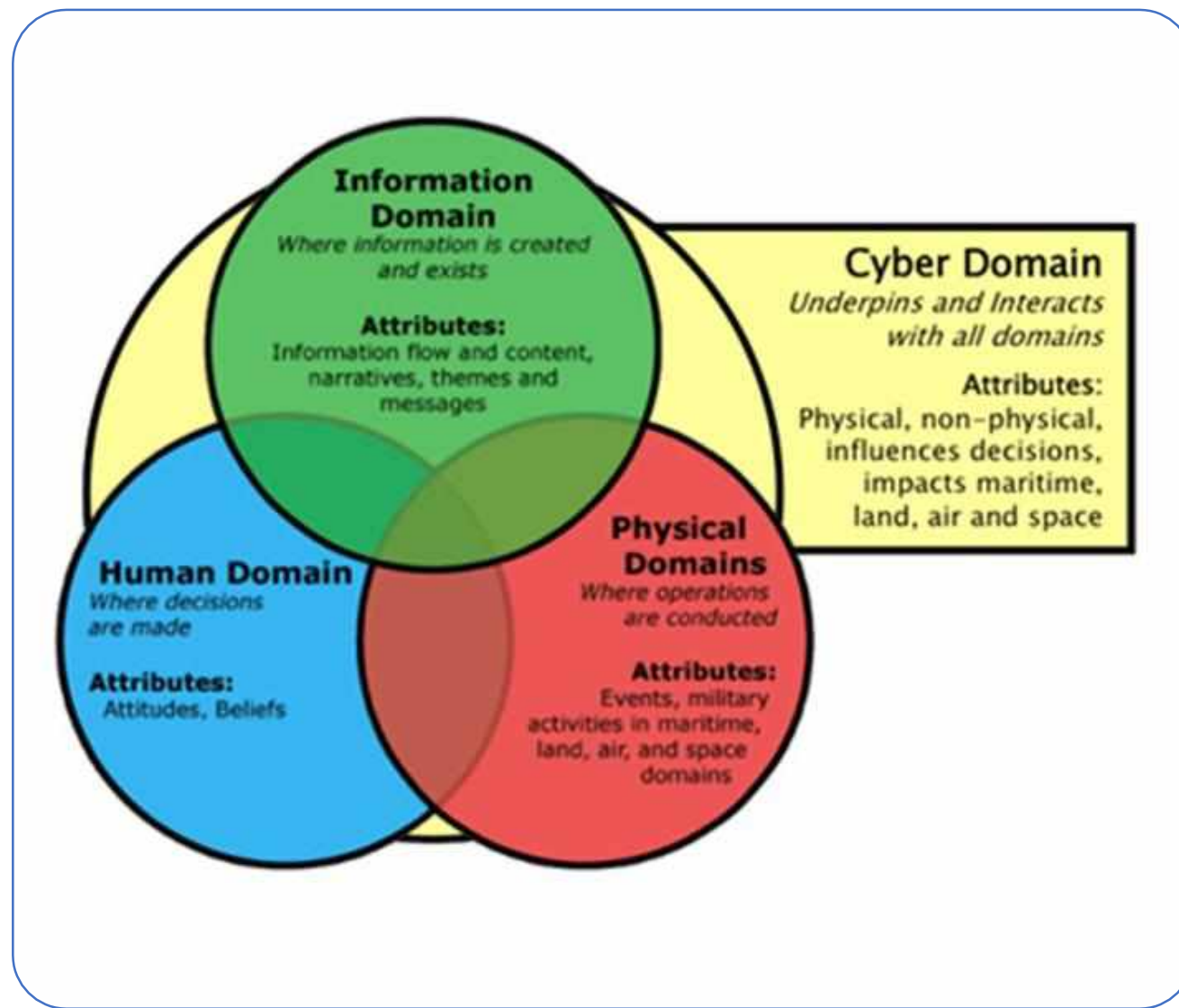
23 октября 2025 года



Мегатренды в информационной безопасности:
куда идем и что делать?

Масалович Андрей Игоревич

Киберпространство (США)



Гибридная война

- ❖ Гибридная война - (англ. hybrid warfare) — вид враждебных действий, при котором нападающая сторона не прибегает к классическому военному вторжению, а подавляет своего оппонента, используя сочетание скрытых операций, диверсий, кибервойны, а также оказывая поддержку повстанцам, действующим на территории противника.
- ❖ «Мы должны научиться защищаться, задерживать, атаковать и маневрировать в киберпространстве, так же, как мы могли бы делать это на земле, на море или в воздухе, и все вместе одновременно.
- ❖ Будущая война всегда будет включать в себя киберизмерение, и оно может стать доминирующей формой» - Генерал Дэвид Ричардс, 2011

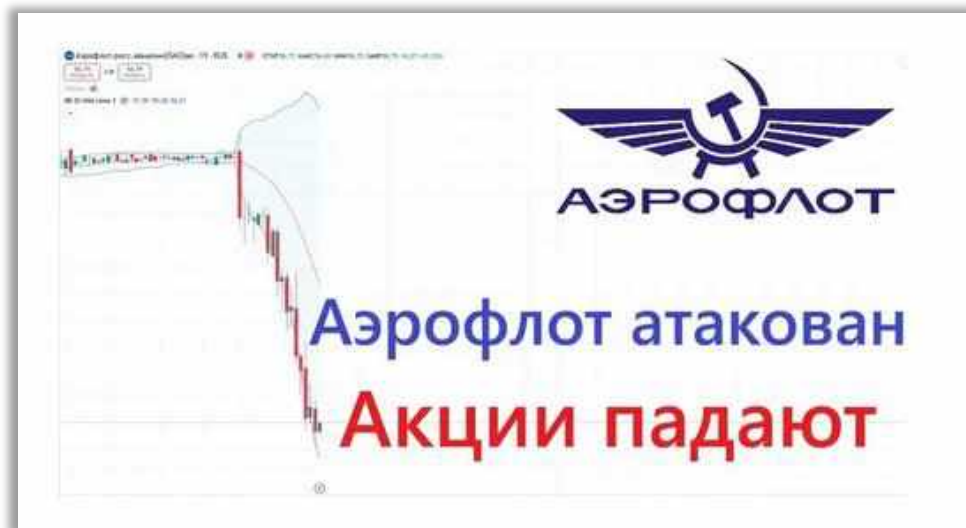
Атака на Аэрофлот: Хронология событий

✂ 27 июля 10:52 — первые сообщения о недоступности мобильного приложения и горячей линии

✂ 28 июля утром — официальное подтверждение IT-сбоя, отмена 54 пар рейсов (42% от запланированных)

✂ 28 июля днем — хакеры взяли на себя ответственность за атаку, заявили о краже 22 ТБ данных

✂ 29-30 июля — восстановление штатного расписания полетов, возбуждение уголовного дела по ст. 272 УК РФ



Источник: <https://t.me/belyaevsec>

Финансовые и репутационные последствия

✎ Прямые убытки:

- ◆ Отмена 54 пар рейсов затронула ~20 тысяч пассажиров.
- ◆ Оценочный ущерб от \$10 до \$50 млн за сутки простоя
- ◆ Падение стоимости акций на фоне негативных новостей

💬 Долгосрочные последствия:

- ☞ Репутационные риски для крупнейшего российского перевозчика
- ☞ Возможные штрафы регуляторов за недостаточную защиту данных
- ☞ Необходимость крупных инвестиций в модернизацию ИБ-систем

⚡️ Правильные действия при реагировании

1. Быстрая изоляция

- ☞ Оперативное отключение скомпрометированных систем
- ☞ Предотвращение дальнейшего распространения атаки

2. Коммуникационная стратегия

- ☞ Прозрачность с пассажирами о сбоях и правах на компенсацию
- ☞ Координация с регуляторами и правоохранительными органами

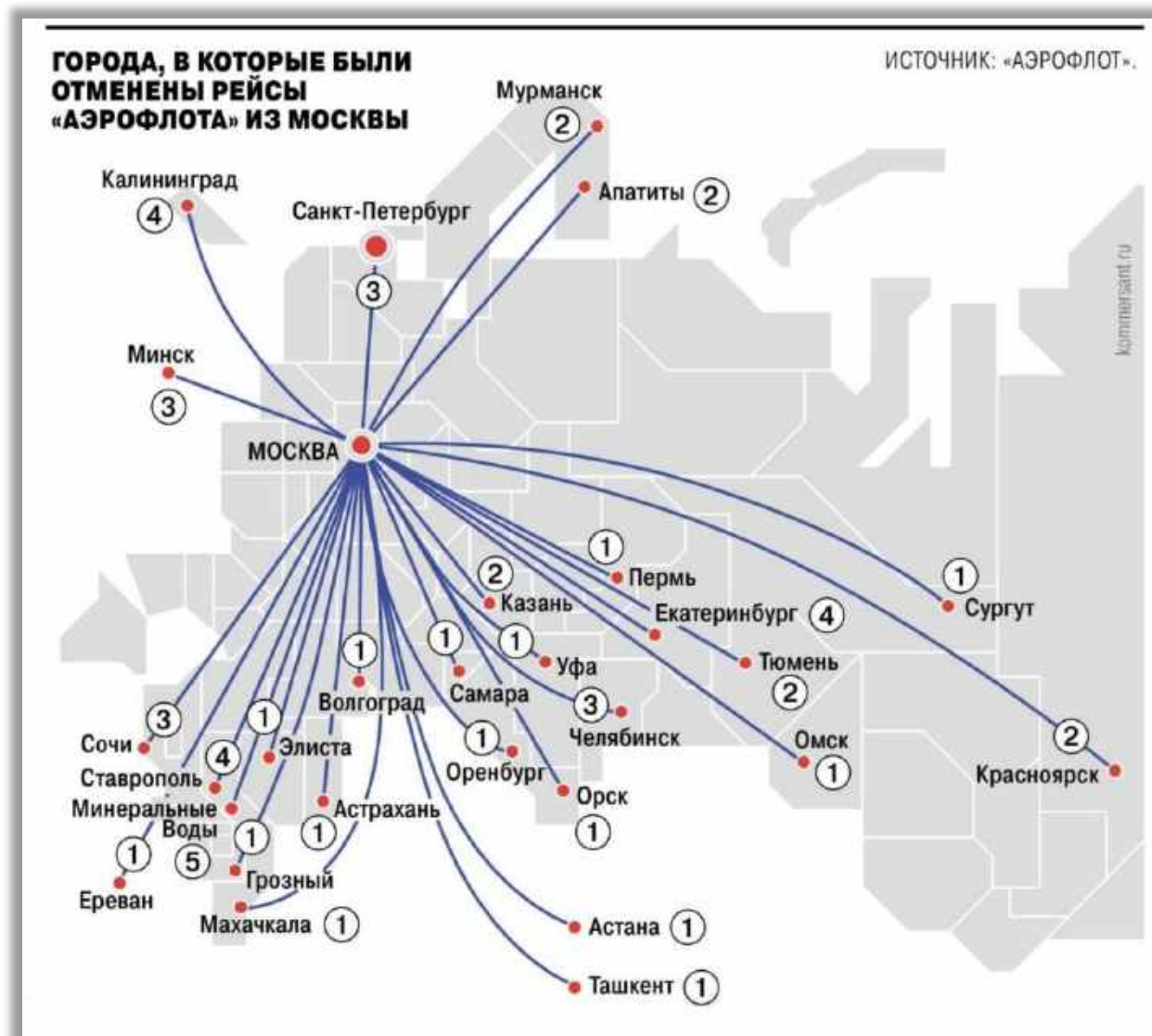
3. Continuity planning

- ☞ Быстрое развертывание альтернативных рабочих мест в Шереметьево
- ☞ Мануальные процессы продажи билетов через кассы
- ☞ Восстановление расписания за 48 часов

4. Вовлечение экспертов

- ☞ Работа с профильными ведомствами и ИБ-партнерами
- ☞ Привлечение внешних экспертов по цифровой криминалистике

⚡ Правильные действия при реагировании



Прошло полтора месяца...



Оперативно-стратегическая аналитика

Прогнозирование
внезапной атаки противника

13 июня – ракетный удар Израиля по Ирану

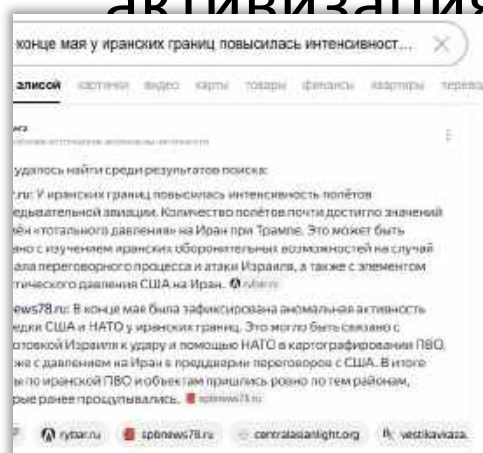


Порядок решения задачи OSINT

- Один: Матрица интересов и угроз
- Два: Конкретная задача
- Три: Разведпризнаки (маркеры)
- Четыре: Контрольные точки в Сети
- Пять: Мониторинг

Пример задачи OSINT: Иран

- **Один:** Нападет Израиль
- **Два:** Ударит ракетами
- **Три:** За 7-14 дней - авиаразведка
- **Четыре:** Рыбарь и др.
- **Пять:** 30 мая – резкая активизация



Основные тренды – 2025.

Угрозы.

Применение искусственного интеллекта (ИИ) в атаках.

Злоумышленники используют генеративные модели для создания фишинговых писем, подделывания голосов руководителей или записи видеосообщений с deepfake-эффектом.

Атаки через цепочку поставок.

Злоумышленники компрометируют менее защищённого подрядчика или программное обеспечение, чтобы проникнуть в крупную цель.

Уязвимости и атаки на публичные сервисы.

Злоумышленники эксплуатируют уязвимости в общедоступных приложениях и сервисах, проникая в сеть и затем проводя сканирование.

Атаки на облачную инфраструктуру.

Массовый переход в облако расширил поверхность атаки: неправильные конфигурации хранилищ, утечки облачных ключей и уязвимости в популярных облачных платформах нередко ведут к крупным инцидентам.

Основные тренды – 2025.

Технологии.

Автоматизация процессов обнаружения угроз и реагирования на инциденты с помощью ИИ.

Алгоритмы машинного обучения анализируют большие объёмы данных, выявляя аномалии и потенциальные угрозы в реальном времени.

Рост популярности решений на основе облачных технологий для защиты данных.

Компании в первую очередь ориентируются на использование облачных технологий для создания, хранения и обработки данных, а традиционные решения рассматриваются только как дополнительный вариант.

Переход к беспарольным технологиям в сфере аутентификации, где биометрия играет ключевую роль.

Например, стандарт FIDO2, получивший поддержку Google, Amazon и Apple, устойчив к широкому спектру атак, связанных с кражей учётных данных.

Основные тренды – 2025. Стратегии.

Комплексный подход к безопасности

Нужна не просто техническая защита, а продуманная архитектура, в которой всё взаимосвязано — от политик доступа до анализа поведения пользователей.

Формирование культуры безопасности

На смену формальному обучению приходят интерактивные тренинги, симуляции атак, геймификация. Людей обучают мыслить как хакеры, чтобы глубже понимать потенциальные угрозы и уязвимости.

Основные тренды – 2025.

Законодательство

Ужесточение регулирования критической информационной инфраструктуры (КИИ).

С 1 января 2025 года вступили в силу поправки в Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Например, расширен перечень субъектов КИИ, обновлены критерии категорирования объектов, ужесточена ответственность за несоблюдение требований по защите КИИ.

Новые стандарты и требования к управлению инцидентами ИБ (ГОСТ Р 58900-2025).

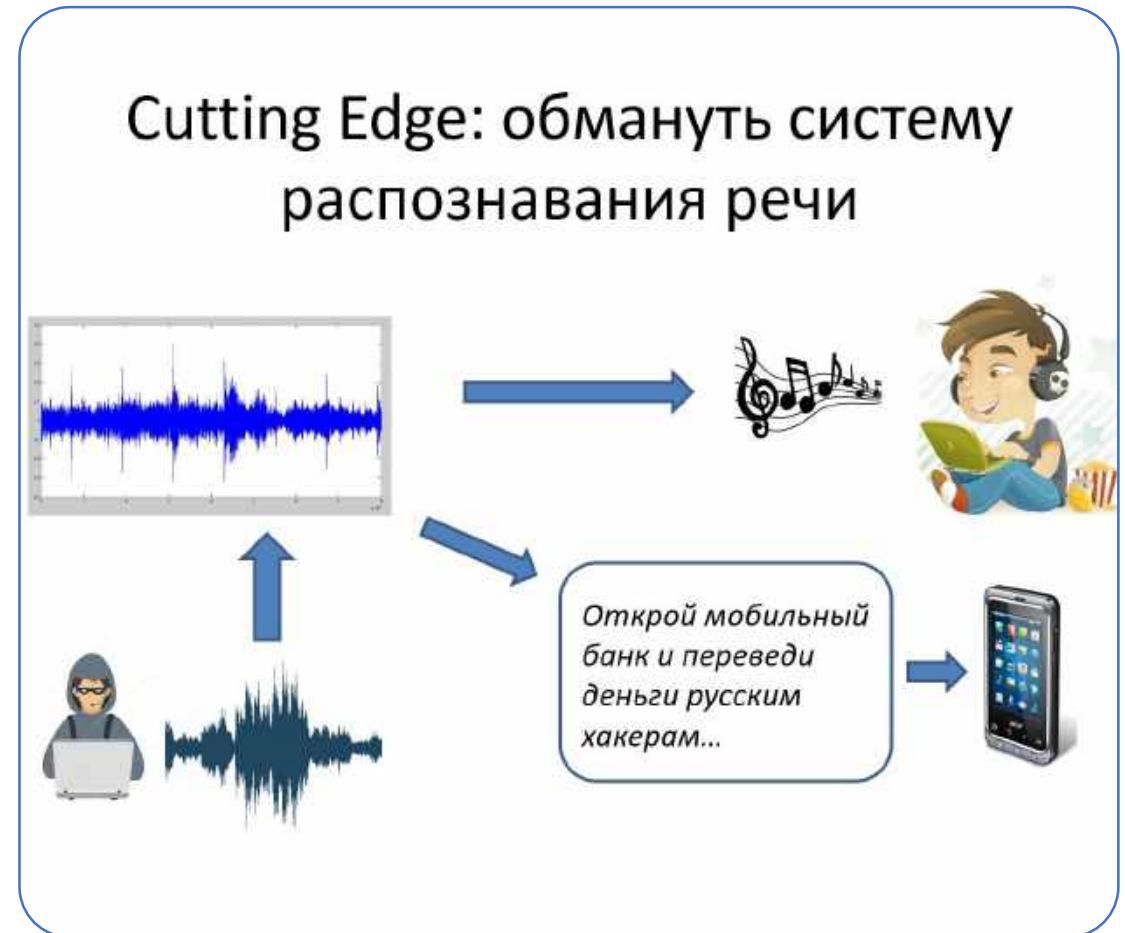
Утверждены обязательность внедрения систем управления информационной безопасностью (СУИБ), журналирование инцидентов и сокращение сроков обязательного уведомления регуляторов и пострадавших лиц о произошедших инцидентах до 24 часов с момента обнаружения.

Будущие тренды ИИ-атак



Атаки на голосовых помощников и "умные" устройства

- ❖ Генерация аудиозапросов, имитирующих голос владельца устройства — для активации функций, совершающих действия от имени пользователя (например, отправка сообщений, транзакции, разблокировка IoT-устройств).
- ❖ Злоупотребление голосовыми интерфейсами в офисах: злоумышленник может использовать записанный или синтезированный голос для управления "умными" конференц-системами или блоками автоматизации.
- ❖ Атаки через акустические сигналы вне слышимого диапазона (так называемые "невидимые команды").



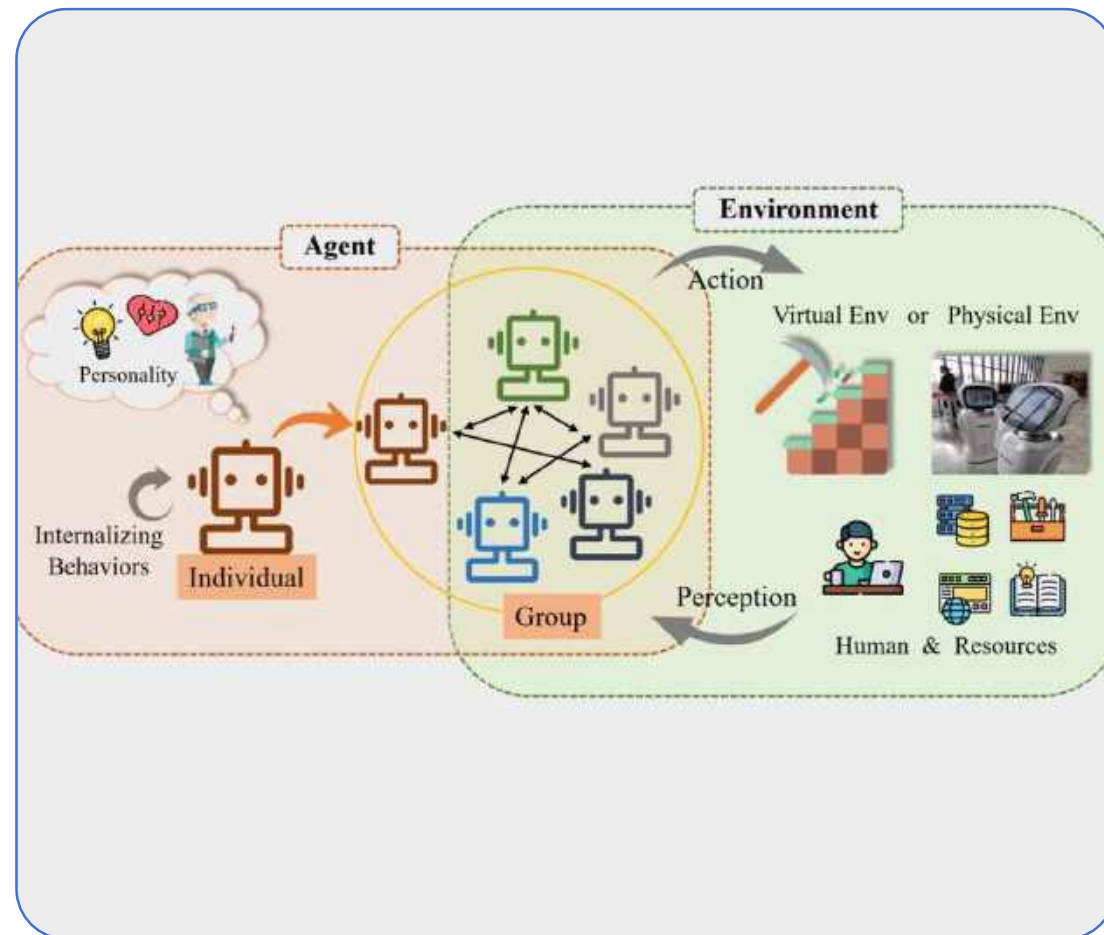
Атаки через IoT и промышленный ИИ

- ❖ ИИ может быть использован для подмены телеметрии и генерации ложных сигналов в системах SCADA.
- ❖ Заражение моделей машинного обучения на заводах "на входе": если ИИ обучен на искажённых данных — он ошибается при управлении станками и процессами.
- ❖ Злоумышленники могут использовать генеративный ИИ для создания "вредных" обновлений программного обеспечения или firmware на устройствах.



Атаки через LLM-агентов и автономные ИИ-скрипты

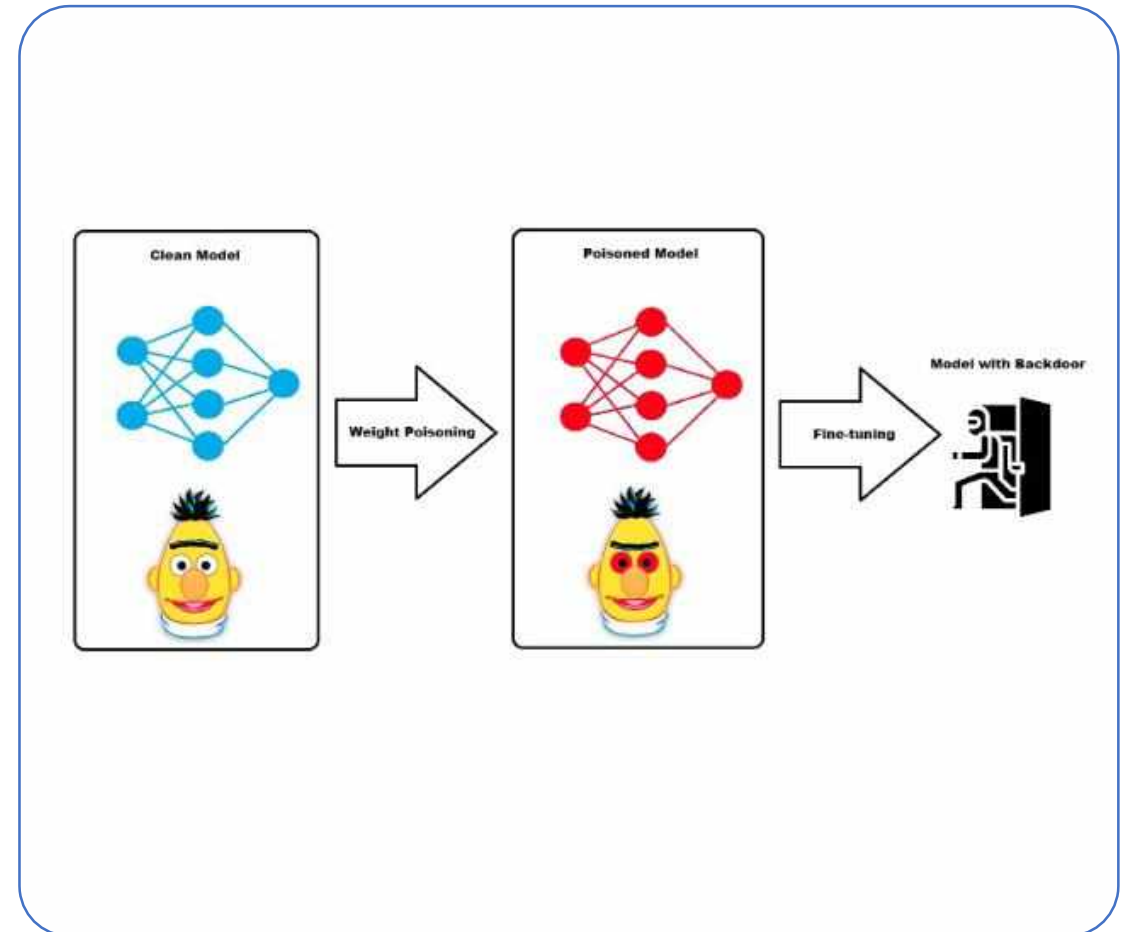
- ❖ ИИ-агенты могут самостоятельно искать уязвимости в коде и отправлять отчёты злоумышленникам.
- ❖ Они способны вести переговоры с поддержкой, притворяясь клиентом, и получать информацию.
- ❖ Интеграция с API позволяет ИИ в реальном времени управлять ботнетами, формировать фишинговые рассылки и атаковать целевые сервисы.



Атаки на ИИ через "отравление" обучающих данных (data poisoning)

Если злоумышленник заранее "заражает" обучающие данные:

- ❖ Модель начинает ошибаться — например, пропускать вредоносные файлы или «принимать» поддельные документы.
- ❖ Возможна подмена предпочтений: в маркетинге, рекомендациях, фильтрации.



Использование синтетических идентичностей

Генеративные модели позволяют создавать абсолютно новые личности: фейковые сотрудники, фейковые клиенты, даже фейковые чиновники. Эти «люди» могут:

- ❖ Получать доступ к сервисам.
- ❖ Формировать доверительные отношения с людьми и организациями.
- ❖ Обманом подписывать документы или участвовать в голосованиях/опросах
- ❖ Пример из прошлого: Алена Писклова (отборочный тур «Мисс Вселенная – 2004», 37929 голосов)



2025: Атака на IoT «Умный дом»

- ❖ В начале 2025 года произошла масштабная атака на миллионы IoT-устройств (умные колонки, камеры, термостаты и даже подключенные автомобили).

Что произошло?

- ❖ Слабая защита устройств, например заводские пароли «по умолчанию», позволила злоумышленникам получить полный контроль.
- ❖ Итог: массовые сбои в работе систем «умного дома», а также основа для создания ботнетов, которые атаковали корпоративные серверы.

Чему это нас учит?

- ❖ Стандарты безопасности для IoT-устройств остаются недостаточными, а пользователи игнорируют обновления и смену паролей.



2025: Атака на энергетическую инфраструктуру

- ❖ Известные хакеры атаковали системы управления энергетическими сетями в нескольких странах Европы. Это привело к временным отключениям электроэнергии в крупных городах, затронув миллионы людей.

Что произошло?

- ❖ Атака была направлена на устаревшие SCADA-системы, которые контролируют энергосети.
- ❖ Используя фишинговые атаки, злоумышленники получили доступ к критически важным системам управления.

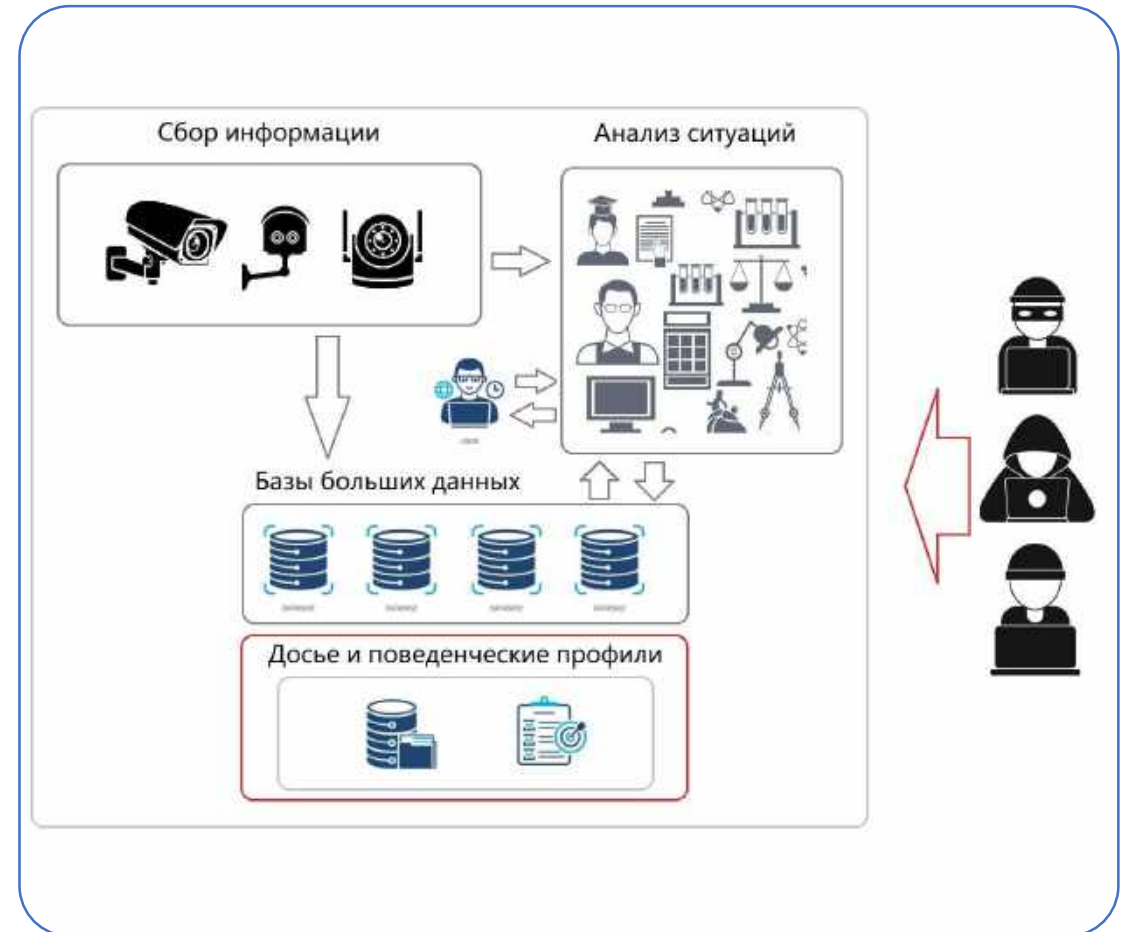
Чему это нас учит?

- ❖ Инфраструктура, от которой зависят жизни миллионов людей, должна быть модернизирована и защищена от фишинговых угроз и взломов.



Атаки на IoT – часть более масштабных атак

- ❖ «Мы должны научиться защищаться, задерживать, атаковать и маневрировать в киберпространстве, так же, как мы могли бы делать это на земле, на море или в воздухе, и все вместе одновременно. Будущая война всегда будет включать в себя киберизмерение, и оно может стать доминирующей формой» - Генерал Дэвид Ричардс, 2011
- ❖ Гибридная война - (англ. hybrid warfare) — вид враждебных действий, при котором нападающая сторона не прибегает к классическому военному вторжению, а подавляет своего оппонента, используя сочетание скрытых операций, диверсий, кибервойны, а также оказывая поддержку повстанцам, действующим на территории противника.



Топ 10 уязвимостей IoT



1. Слабые, угадываемые или жестко вшитые пароли

Слабые, угадываемые или жестко закодированные пароли

Использование:

- ❖ • Легко поддаются перебору
- ❖ • Общедоступны
- ❖ • Неизменяемые учетные данные

Включают бэкдоры в прошивке или клиентское программное обеспечение, которые предоставляют несанкционированный доступ.



2. Небезопасные сетевые службы

Ненужные или небезопасные сетевые службы, работающие на самом устройстве, особенно:

- ❖ Те, которые открыты для доступа в Интернет
- ❖ Любые, которые ставят под угрозу конфиденциальность, целостность /подлинность или доступность информации
- ❖ Любая служба, которая допускает несанкционированное удаленное управление

```
Host is up (0.00051s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
```

3. Небезопасные интерфейсы экосистемы

Небезопасные интерфейсы в экосистеме за пределами устройства:

- ❖ Веб
- ❖ API бэкэнда
- ❖ Облако
- ❖ Мобильные устройства

Распространенные проблемы:

- ❖ Отсутствие аутентификации
- ❖ Отсутствие авторизации
- ❖ Отсутствие или слабое шифрование
- ❖ Отсутствие фильтрации ввода и вывода

A1:2017-Injection

A2:2017-Broken Authentication

A3:2017-Sensitive Data Exposure

A4:2017-XML External Entities (XXE)

A5:2017-Broken Access Control

A6:2017-Security Misconfiguration

A7:2017-Cross-Site Scripting (XSS)

A8:2017-Insecure Deserialization

A9:2017-Using Components with Known Vulnerabilities

4. Отсутствие механизма безопасного обновления

Отсутствие возможности безопасного обновления устройства.

- ❖ Отсутствие проверки прошивки на устройстве
- ❖ Отсутствие безопасной доставки (незашифрованная при передаче)
- ❖ Отсутствие механизмов предотвращения отката
- ❖ Отсутствие уведомлений об изменениях безопасности из-за обновлений



5. Использование небезопасных или устаревших компонентов

Использование устаревших или небезопасных программных компонентов/библиотек, которые могут привести к взлому устройства.

- ❖ Небезопасная настройка платформ операционной системы
- ❖ Сторонние программные библиотеки из скомпрометированной цепочки поставок
- ❖ Сторонние аппаратные компоненты из скомпрометированной цепочки поставок



Meltdown



Spectre

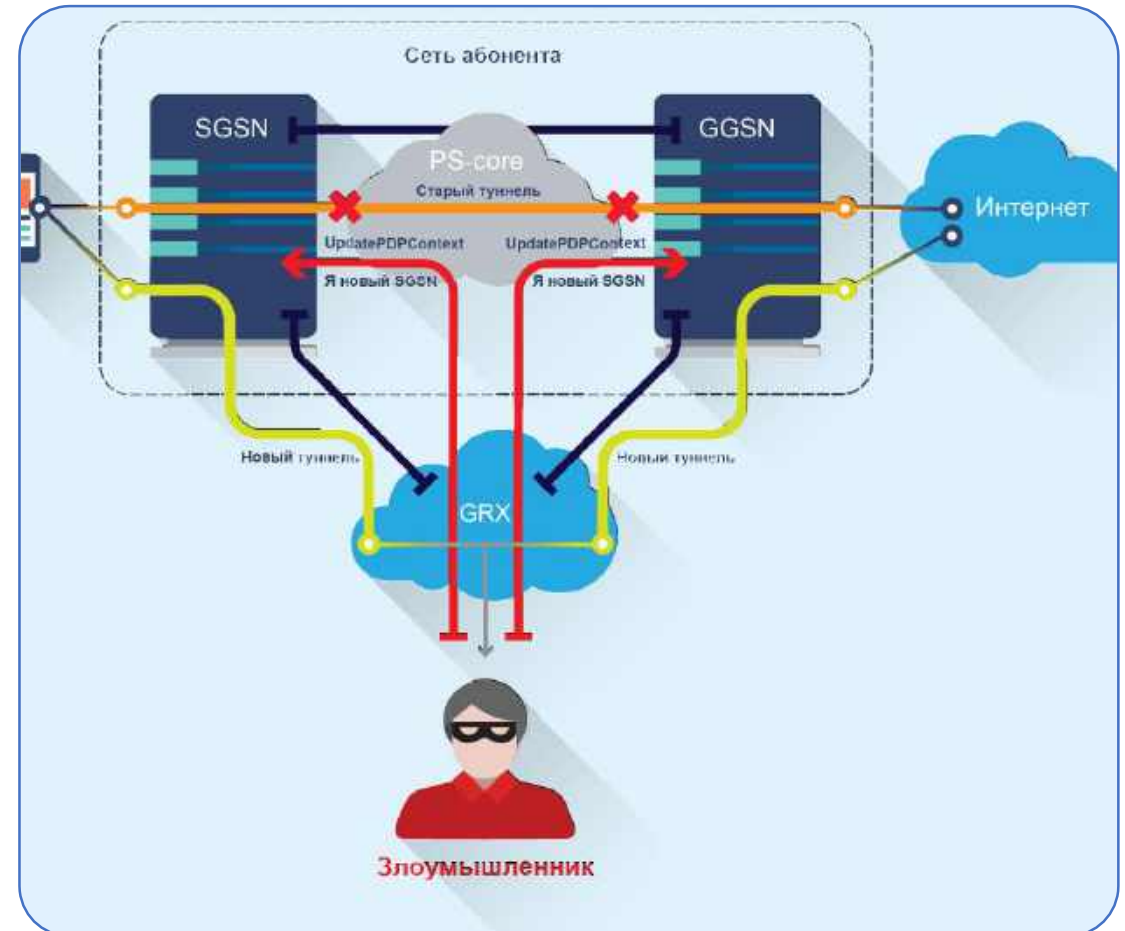


Heartbleed

6. Недостаточная защита конфиденциальности

Персональная информация пользователя, хранящаяся на устройстве или в экосистеме, которая используется небезопасно, ненадлежащим образом или без разрешения.

Исследование Корнелльского университета 2017 г.: «Умный дом — не крепость. Мы изучаем устройства умного дома IoT и обнаруживаем, что их показатели сетевого трафика могут раскрывать потенциально конфиденциальные взаимодействия пользователя, даже если трафик зашифрован»



7. Небезопасная передача и хранение данных

Отсутствие шифрования или контроля доступа к конфиденциальным данным где бы то ни было в экосистеме, в том числе при хранении, передаче или во время обработки.

«Согласно сайту по сборке прошивок nodeMCU-builds, за последние 60 дней было 13 341 пользовательских сборок прошивок для этой платформы. Из них только 19% имеют поддержку SSL, а 10% включают модуль криптографии».



8. Отсутствие управления устройствами

Отсутствие поддержки безопасности на устройствах, развернутых в производстве, включая управление активами, управление обновлениями, безопасный вывод из эксплуатации, мониторинг систем и возможности реагирования.

- 25% по-прежнему используют Excel
- 56% проверяют местоположение активов только один раз в год, а 10-15% - раз в 5 лет
- Персонал тратит более 10 часов в неделю на решение проблем с точностью данных
- Почти 66% ИТ-менеджеров имеют неполные записи своих ИТ-активов



9. Небезопасные настройки по умолчанию

Устройства или системы, поставляемые с небезопасными настройками по умолчанию или не имеющие возможности сделать систему более безопасной, ограничив операторов от изменения конфигураций.

- ❖ Неправильные разрешения файловой системы
- ❖ Открытые службы, работающие как root



10. Отсутствие физической защиты

Отсутствие мер физической защиты, позволяющее потенциальным злоумышленникам получить конфиденциальную информацию, которая может помочь в будущей удаленной атаке или получить локальный контроль над устройством.



Выбор Кибердеда: *взлом шлагбаума*

- ❖ В системе управления преимущественно придомовыми шлагбаумами Москвы была обнаружена опасная уязвимость.
- ❖ Речь идет о трети всех установленных шлагбаумов в Москве, более 1500 штук.
- ❖ Причина - уязвимость системы авторизации в веб-приложении, которая позволяет при минимальных правах доступа с демо-аккаунта получать информацию о любых объектах системы и открывает возможность управлять ими.

Postuf 29 дек 2021 в 15:00

Как открыть 1500 шлагбаумов Москвы

5 мин 137К

Блог компании Postuf, Информационная безопасность*

Прогноз 2021

Случилось как-то, что рядом с офисом Postuf жильцы соседнего дома поставили себе шлагбаум. С парковкой в центре Москвы и так проблемы, а если еще и офисное здание неподалеку, в общем, жильцов можно понять. Но не давало покоя ощущение, что доступ к шлагбаумам могут получить далеко не только жильцы дома.

Стало интересно, кто вообще занимается установкой шлагбаумов и насколько активно. Для этого выходим из офиса на улицу и проводим разведку по открытым источникам на местности.



Компания, установившая шлагбаум

Что делать? Учиться!



Клуб Кибердеда



Главный тренд – утрата цифровой приватности



Спасибо!



Масалович Андрей Игоревич

Ака Кибердед

Телеграм-канал: Кибердед_official

Сайт: am.news

E-mail: avalanche100500@gmail.com

