НОВИКОМ

2024 Инженеры будущего

КИБЕРБЕЗОПАСНОСТЬ

Обеспечение киберустойчивости России и активное противодействие угрозам в киберпространстве

А.В. Сергеев

Советник, доцент МИЭМ НИУ ВШЭ

И.В. Семичаснов

Директор Центра управления проектными разработками МИЭМ НИУ ВШЭ

КИБЕРБЕЗОПАСНОСТЬ:
Рост атак на физические лица

Одним из главных киберпреступлений считается телефонное мошенничество, которое в России приобрело масштабы национального бедствия

В каждой группе мошенников есть специалисты по сбору и анализу персональных данных (т.н. OSINT), фишингу, автоматизации финансовых операций и т.п.

*Согласно ранее опубликованным материалам ЦБ, банки РФ в 2023 году **предотвратили мошеннические хищения на 5,8 трлн рублей**, но злоумышленники смогли **провести 1,17 млн успешных операций**, что на **33% больше, чем в 2022** году, и украсть **15,8 млрд рублей***

Председатель Банка России Эльвира Набиуллина в ходе форума "Кибербезопасность в финансах"

15,8 млрд. млрд. рублей

Потери россиян от хищения денежных средств в 2023 году

В 46 раз

Увеличилось количество киберпреступлений за 2013-2020 гг.

23%

Снижение раскрываемости за 2020 г.

По данным АО Сбербанк и Банка России

КИБЕРБЕЗОПАСНОСТЬ:
Рост атак на физические лица

Россияне сами оставляют свои данные в Интернет на многочисленных фишинговых сайтах из-за **низкого уровня киберграмотности**

Хакерские сайты (т.н. даркнет) – основная площадка мошенников

Персональные данные, данные о кредитных картах, аккаунтах, действиях в Интернет активно покупаются и продаются, в т.ч. для информационной базы по реализации атак на граждан.

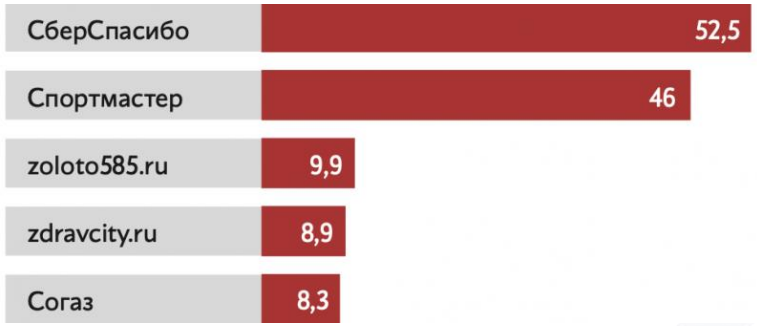
Фишинг (от англ. fishing – рыбная ловля) представляет собой противоправное действие, совершаемое с целью заставить то или иное лицо поделиться своей конфиденциальной информацией, например паролем или номером кредитной карты

>100 млн персональных записей данных россиян попали в сеть в 2020 году

100+ тыс./сутки среднее число звонков мошенников гражданам РФ

13 тыс. объявлений

обнаружили специалисты ЦБ в Интернет о продаже персональных данных россиян



По данным АО Сбербанк, ФинЦЕРТ Банка России, DLBI, 2023

НАКАЗАНИЕ ЗА КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

Неправомерные действия инсайдера	***Преступные действия инсайдера***	***Дропперство***
Сисадмин оборонного предприятия подключил закрытую сеть предприятия к сети Интернет, чтобы скачать СЗИ FreeRADIUS	*Мобильный пробив данных абонентов крупного оператора мобильной связи*	*Студент отдал свою карту и реквизиты для использования мошенниками*
Утечки данных и ущерба не было	***Доказано менее 10 случаев***	***Банк заблокировал транзакцию, ущерба не было***
Статья 274.1 УК РФ **1,5 ГОДА**	**Статья 272 УК РФ, ч. 3** **2 ГОДА**	**Статья 159 УК РФ, ч. 3** **3 ГОДА**

Данные из Баз судов общей юрисдикции

Наиболее часто применяемые статьи УК за компьютерные преступления

272 УК РФ: Неправомерный доступ к компьютерной информации

273 УК РФ: Создание, использование и распространение вредоносных компьютерных программ

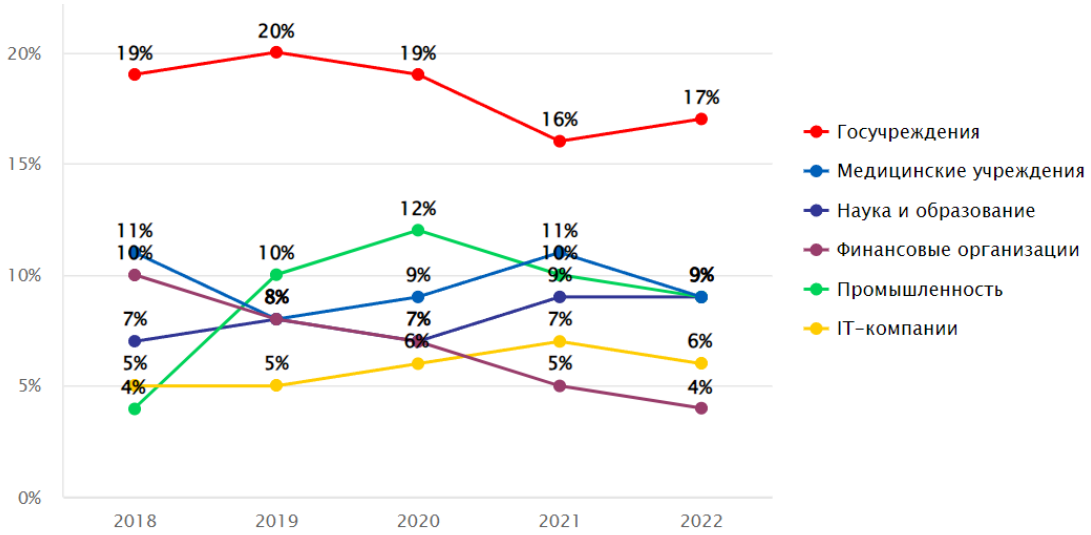
274.1 УК РФ: Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

274.2 УК РФ: Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования

187 УК РФ: Неправомерный оборот средств платежа

РОСТ АТАК НА ПРОМЫШЛЕННЫЕ ОБЪЕКТЫ

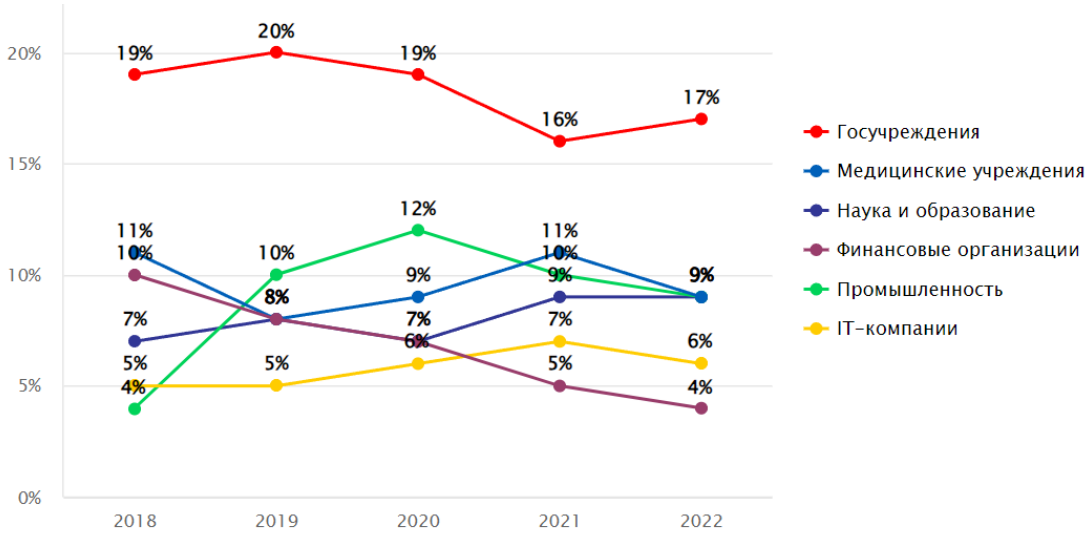
Доля атак на промышленные организации
(от общего числа атак на организации)

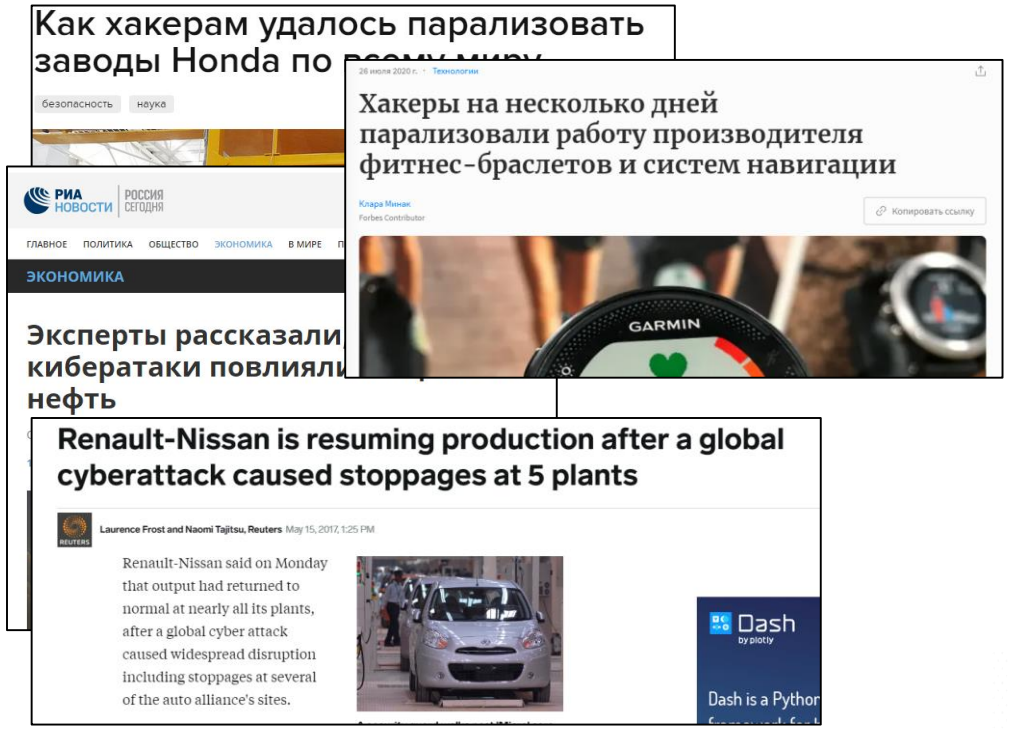


Прогнозы на 2024 год:
в прицеле — предприятия, связанные с государством

РОСТ АТАК НА ПРОМЫШЛЕННЫЕ ОБЪЕКТЫ

Доля атак на промышленные организации
(от общего числа атак на организации)

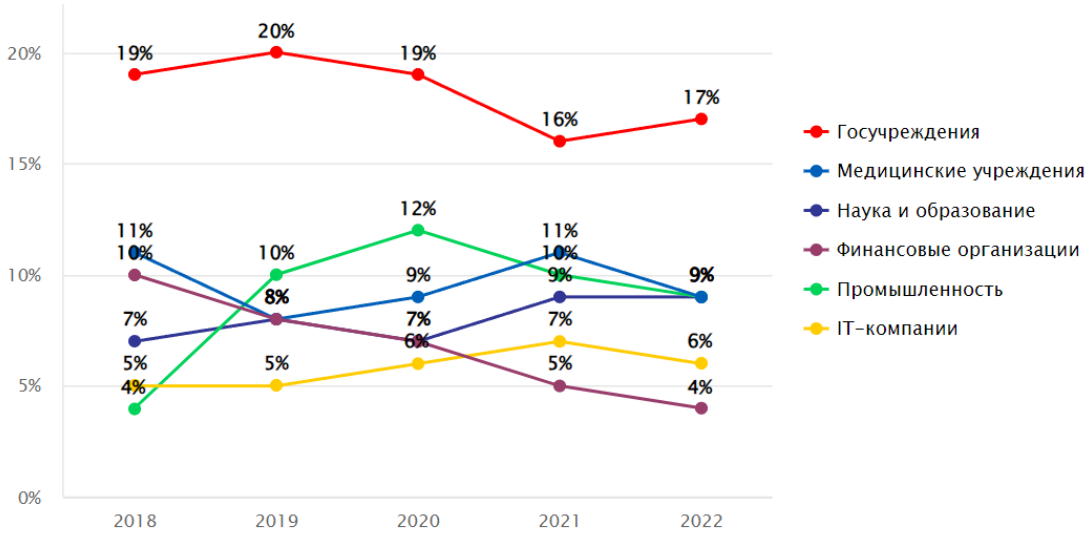


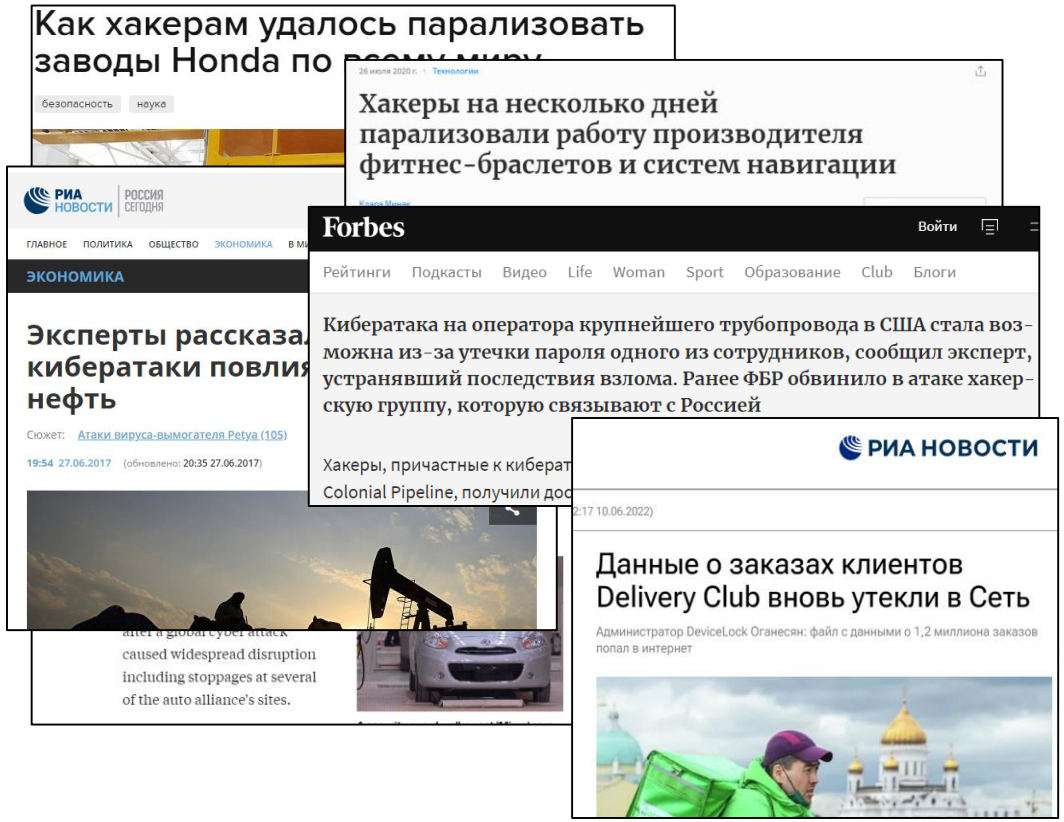


Прогнозы на 2024 год:
в прицеле — предприятия, связанные с государством

РОСТ АТАК НА ПРОМЫШЛЕННЫЕ ОБЪЕКТЫ

Доля атак на промышленные организации
(от общего числа атак на организации)



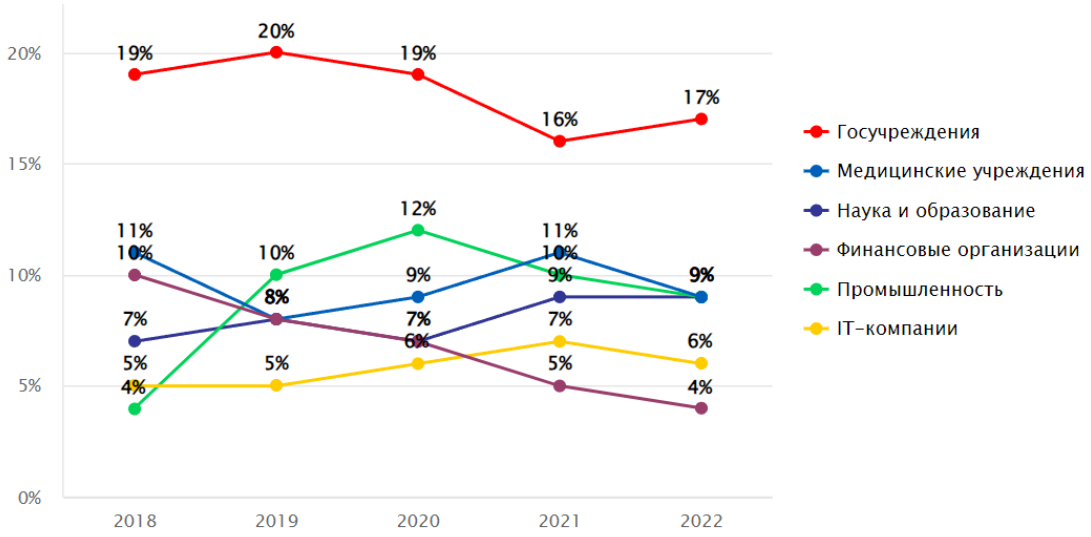


Прогнозы на 2024 год:
в прицеле — предприятия, связанные с государством

Инженеры будущего

РОСТ АТАК НА ПРОМЫШЛЕННЫЕ ОБЪЕКТЫ

Доля атак на промышленные организации
(от общего числа атак на организации)

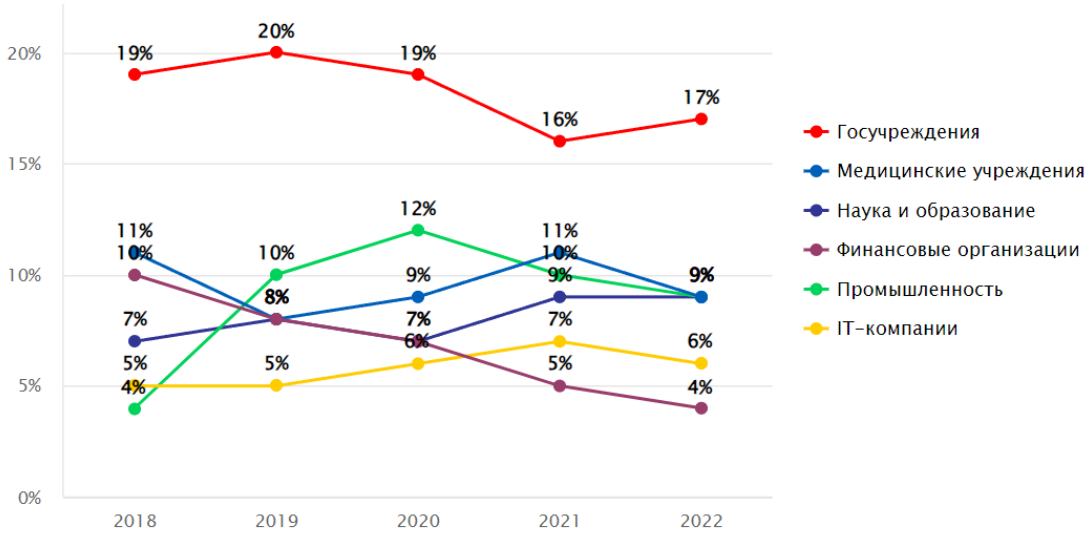


Прогнозы на 2024 год: в прицеле — предприятия, связанные с государством

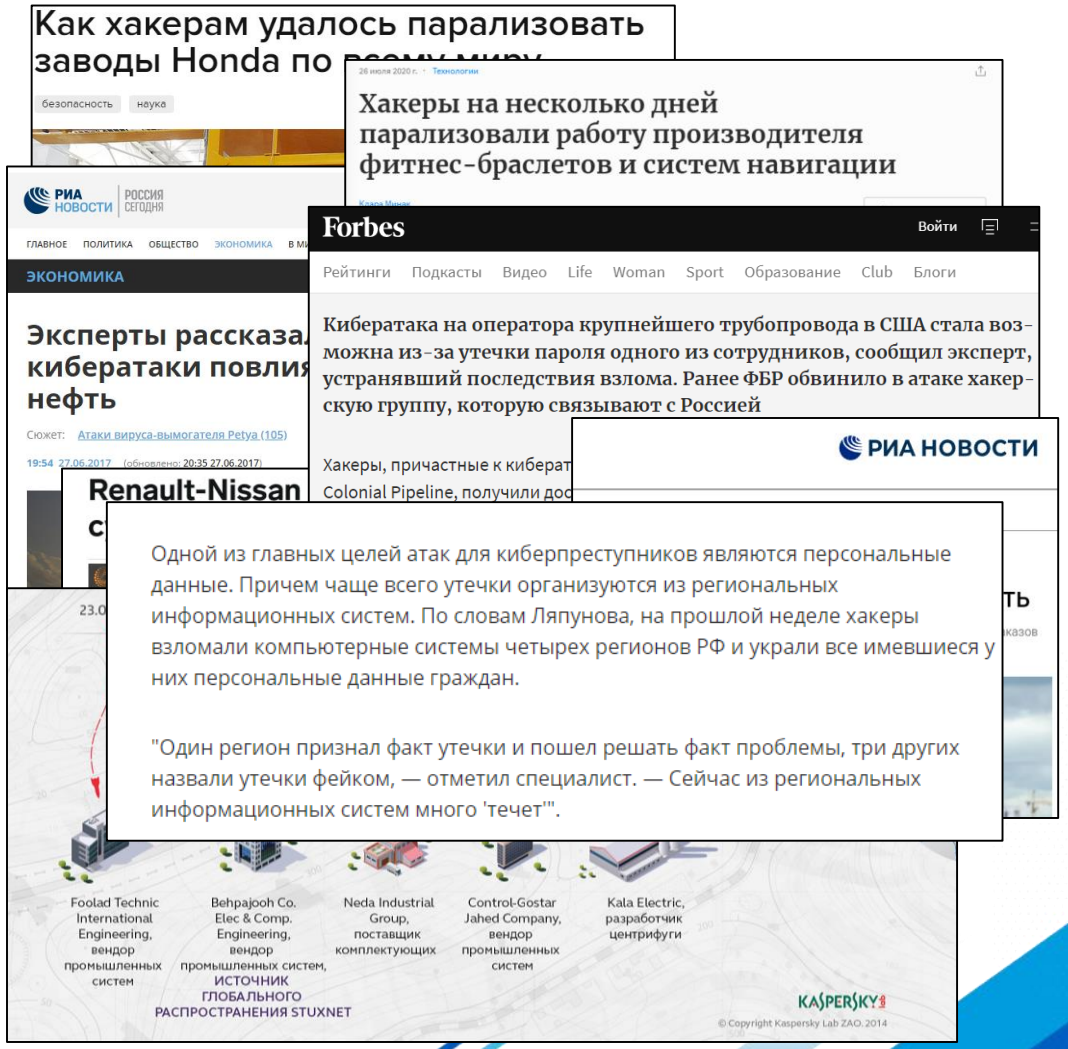
Инженеры будущего

РОСТ АТАК НА ПРОМЫШЛЕННЫЕ ОБЪЕКТЫ

Доля атак на промышленные организации
(от общего числа атак на организации)

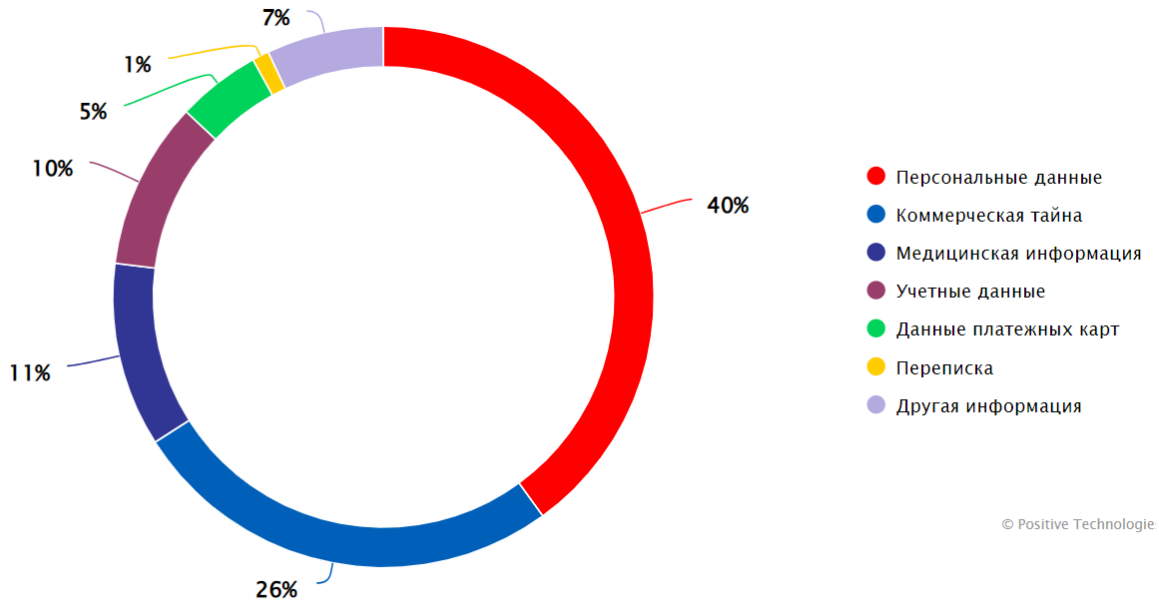


Прогнозы на 2024 год:
в прицеле — предприятия, связанные с государством

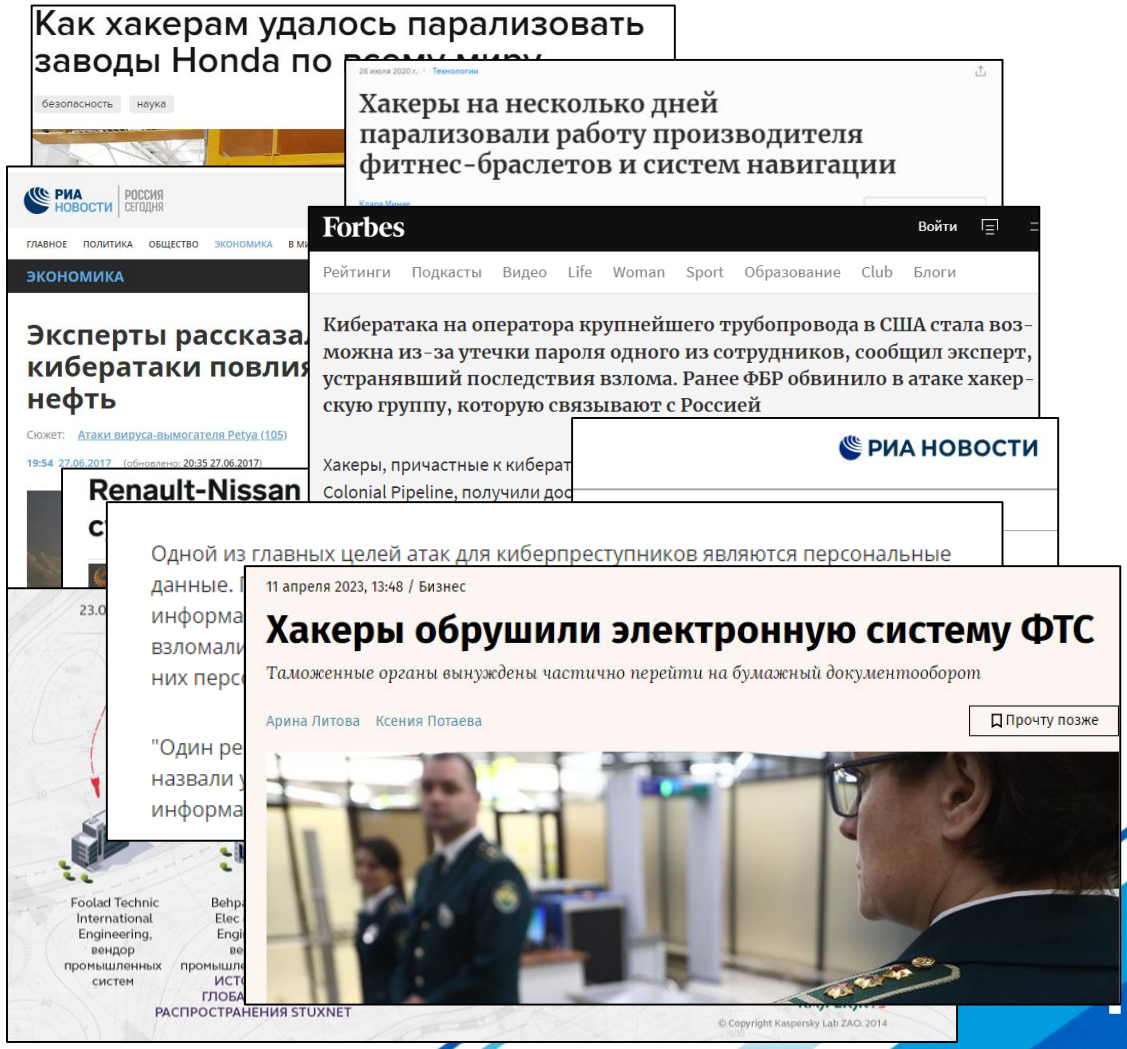


РОСТ АТАК НА ПРОМЫШЛЕННЫЕ ОБЪЕКТЫ

Успешные атаки по типам данных



Прогнозы на 2024 год:
в прицеле — предприятия, связанные с государством



УГРОЗЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЕ ГОСУДАРСТВА И БИЗНЕСА

*«Все последние годы мы отмечаем рост **угроз в сфере информационной безопасности**. И на прошлогодней коллегии предметно говорили об участившихся случаях масштабных и скоординированных кибератак»*

***В.В. Путин** на Коллегии ФСБ, 2020*

«Спецслужбы иностранных государств ищут уязвимые места в информационной инфраструктуре России для совершения массированных кибератак»

***Н. Патрушев**, секретарь Совбеза РФ*

*«Мы считаем, что сфера кибербезопасности является **чрезвычайно важной в мире вообще** и для США, в частности, и для России тоже, в таком же объеме»*

***В.В. Путин** на встрече в президентом США Джо Байденом, июнь 2021*

*«Отсутствие результативности ВСУ может подтолкнуть горячие головы к применению американского **наступательного кибероружия** для нанесения ущерба государственному и военному управлению, экономической системе России»*

*Замсекретаря Совета безопасности (СБ) РФ **Олег Храмов***

В перспективе, основную угрозу государству и обществу несут атаки на промышленные объекты, в первую очередь предприятия ТЭК, производственные цепочки, логистические предприятия

По данным ТАСС

APT-АТАКИ

25%

Ежегодный рост числа атак на системы АСУ-ТП

58,9%

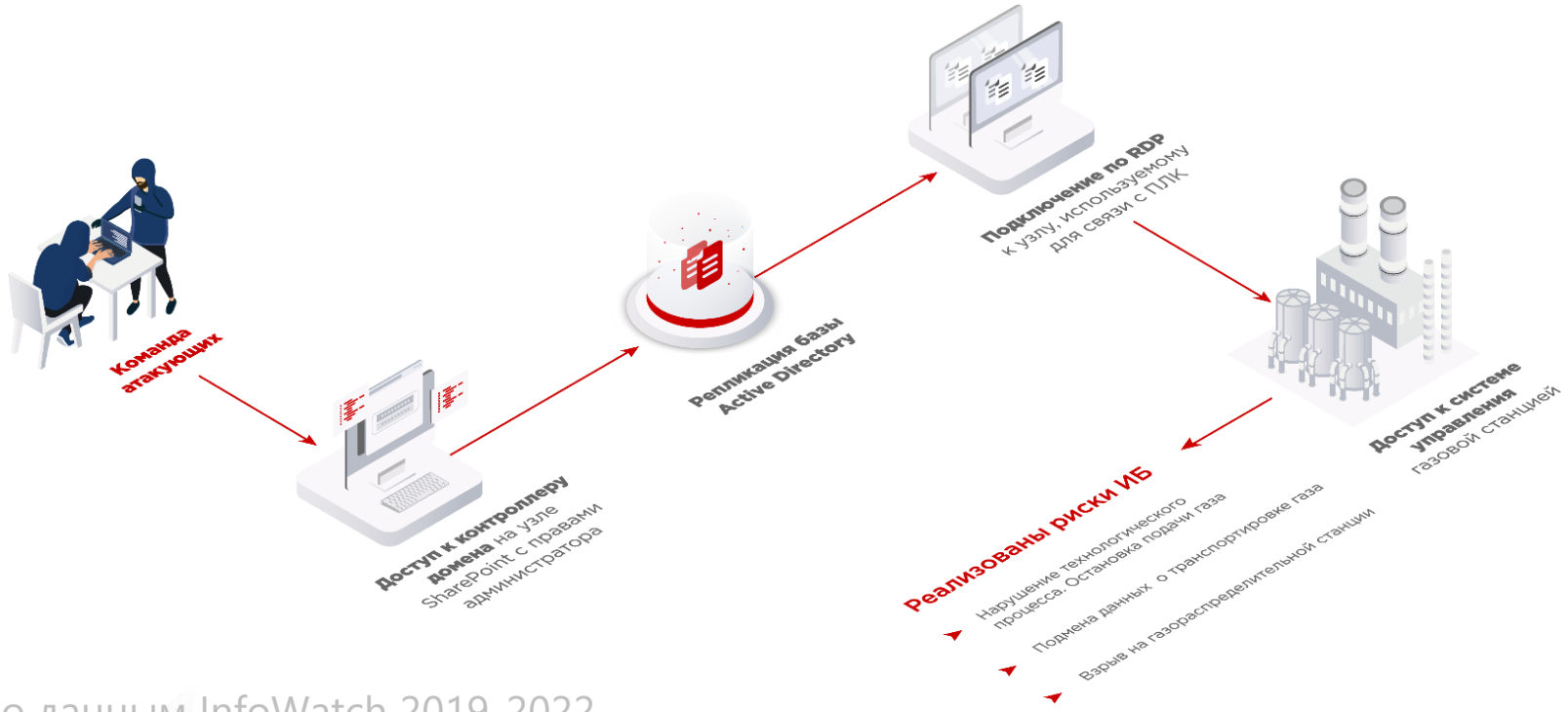
Рост атак на объекты ТЭК

Цель 25%

всех APT-атак в России – объекты ТЭК

Для сложных, целевых, хорошо организованных атак есть специальный термин:

advanced persistent threat (APT-атака)

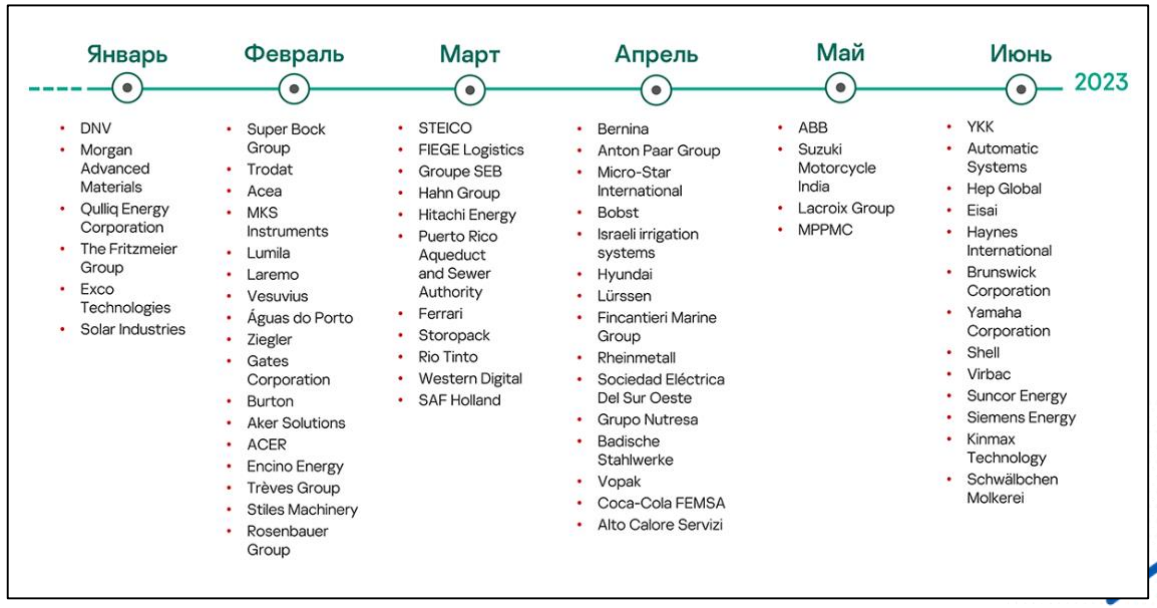


По данным InfoWatch 2019-2022

УГРОЗЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЕ ГОСУДАРСТВА И БИЗНЕСА: Тренды

Вымогатели останутся бичом № 1 промышленных предприятий

Атаки вымогателей на крупные организации или «уникальных» поставщиков будут приводить к тяжёлым последствиям



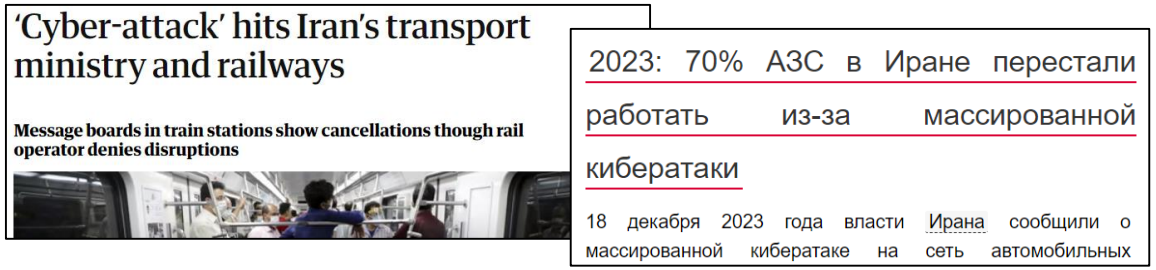
ИБ не поспевает за цифровизацией.
Но темпы развития ИБ разных отраслей и стран отличается

По данным Kaspersky Lab

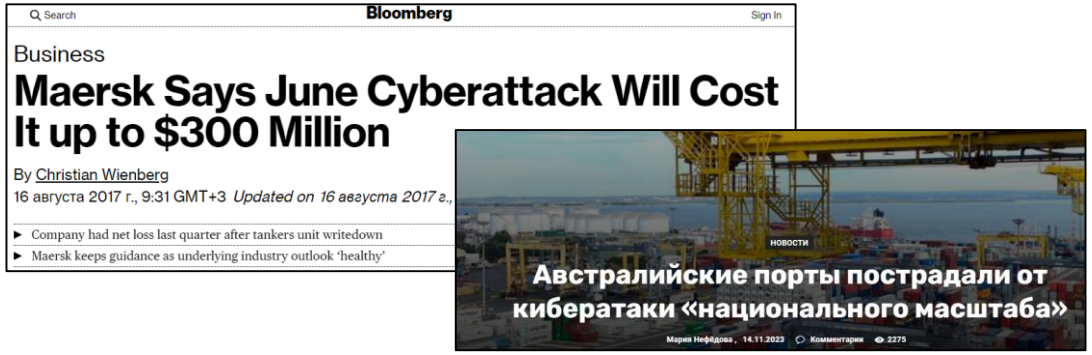
Инженеры будущего

УГРОЗЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЕ ГОСУДАРСТВА И БИЗНЕСА: Тренды

Действия политически мотивированных хактивистов будут иметь более разрушительные последствия



Атаки на логистические и транспортные компании будут нацелены на транспортные средства (а не ИТ-инфраструктуру)



Наступательная кибербезопасность (offensive cybersecurity) становится нормой

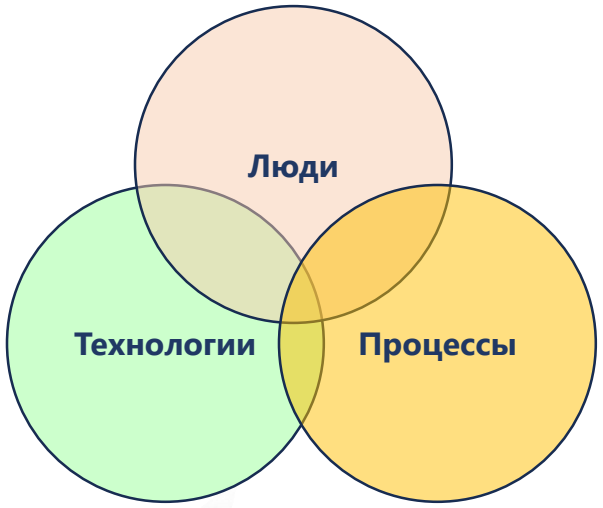
По данным ТАСС

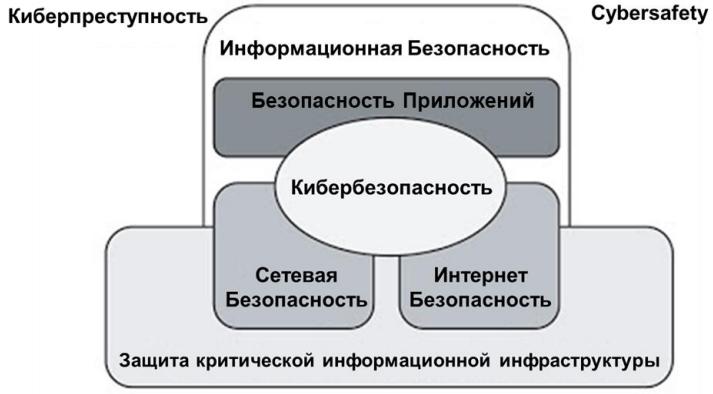
Инженеры будущего

КИБЕРБЕЗОПАСНОСТЬ: междисциплинарный подход

Кибербезопасность –

– это реализация мер по защите систем, сетей и программных приложений от цифровых атак.





Инженеры будущего

ТЕХНОЛОГИЧЕСКИЙ СУВЕРЕНИТЕТ

Российская Федерация – одна из немногих стран,
разрабатывающая **весь спектр систем защиты информации**

В Глобальном индексе кибербезопасности (GCI) Международного союза электросвязи (МСЭ) 2021 Россия **на 5-ом месте**

INFOWATCH
KASPERSKY lab
infotecs
SOLAR
ARMA IF
PT POSITIVE TECHNOLOGIES
Jet
КОД БЕЗОПАСНОСТИ
BI.ZONE Cybersecurity

БАЗОВЫЕ ПОНЯТИЯ:
Аналогия при физической атаке

Угроза

Инструментарий **злоумышленника**, возможный способ (сценарии) реализации угрозы безопасности

Атака
(реализация угрозы)

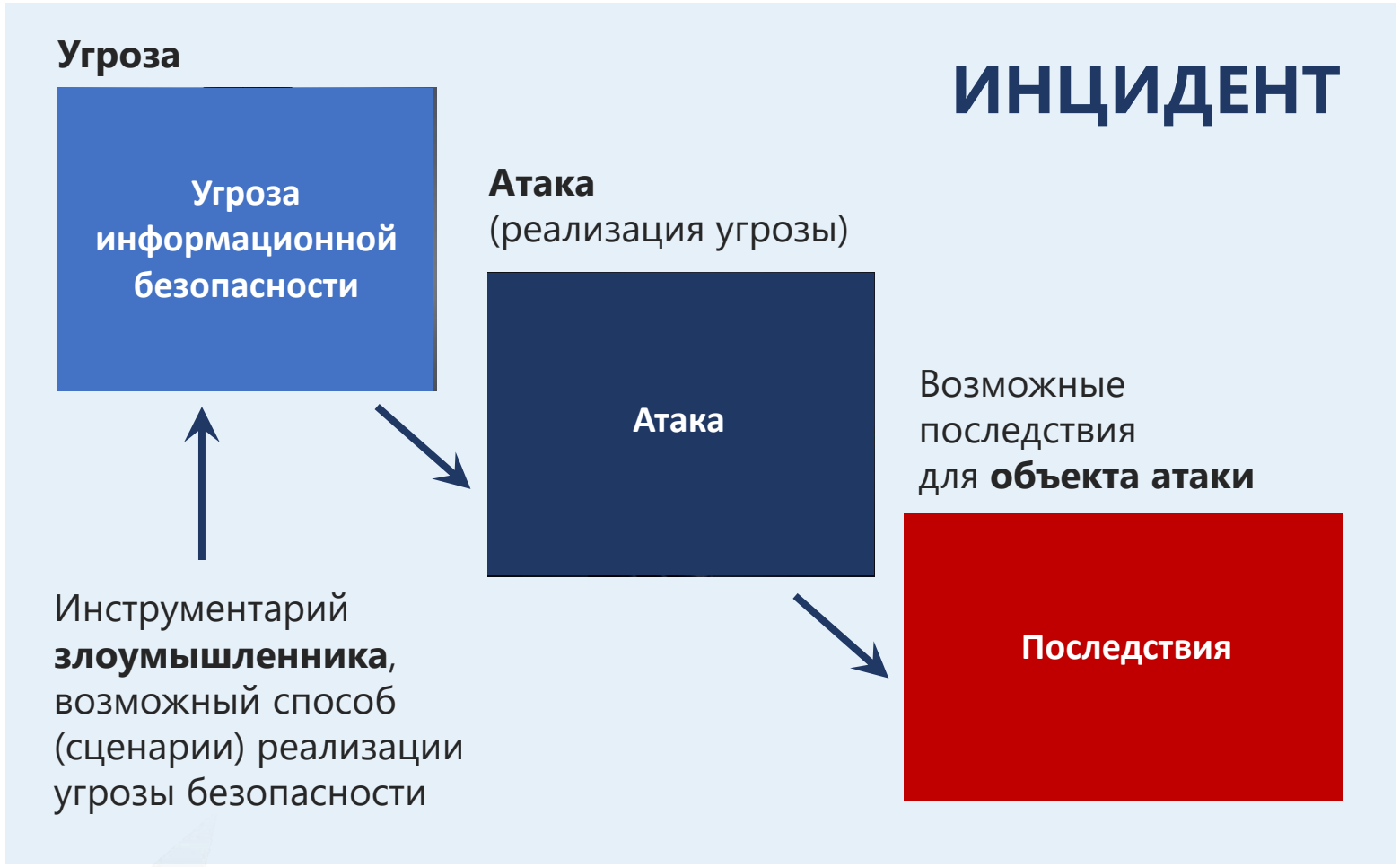
ИНЦИДЕНТ

Возможные последствия для **объекта атаки**

УЯЗВИМОСТЬ

Слабая физическая подготовка, состояние алкогольного опьянения и т.п.

КИБЕРУГРОЗА- КИБЕРАТАКА- ПОСЛЕДСТВИЯ. Пример



УЯЗВИМОСТЬ

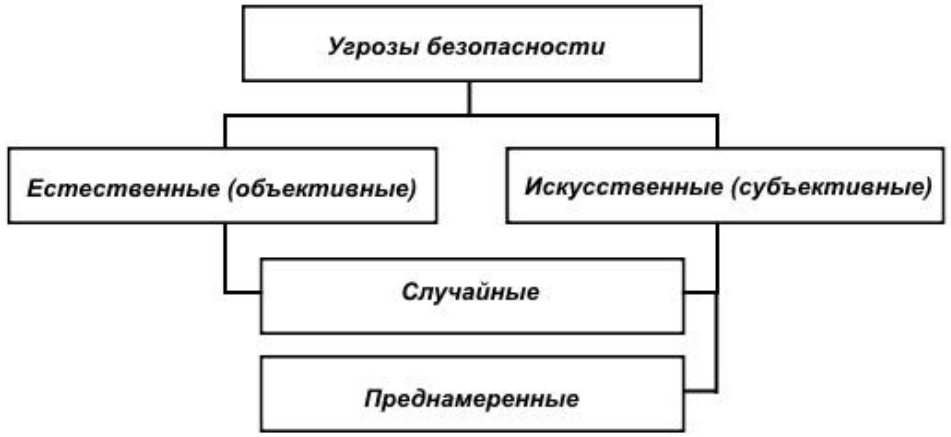
- Некорректная настройка средств защиты, устаревшие версии систем
- Отключение антивируса
- Халатность персонала (переход по фишинговым ссылкам, запуск вредоносного ПО) и т.п.

Слабая физическая подготовка, состояние алкогольного опьянения и т.п.

БАЗОВЫЕ ПОНЯТИЯ: Угрозы, Уязвимости, Атаки

Угроза информационной безопасности – потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию, ее носители и процессы обработки может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

Нарушение безопасности или атака – реализация угрозы безопасности.



Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Уязвимость – свойство системы, которое может привести к нарушению ее защиты при наличии угрозы

Информационная безопасность организации – состояние защищенности интересов организации в условиях угроз в информационной сфере (ГОСТ Р 53114-2008)

Источник угрозы безопасности информации – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

БАЗОВЫЕ ПОНЯТИЯ: Угрозы, Уязвимости, Атаки

Информационная безопасность — важнейшая часть стратегии национальной безопасности

Новый национальный приоритет – информационная безопасность (ИБ) – впервые вошёл в обновлённую стратегию национальной безопасности России, которую в 2021 году подписал президент страны Владимир Путин.

РЕГУЛЯТОРЫ

Национальный проект «Экономика данных»

- Сбор данных
- Передача данных и развитие систем связи
- Хранение данных
- Безопасность данных
- Стандарты и протоколы работы с данными
- Обработка и анализ данных, репозитории открытого кода

О безопасности критической информационной инфраструктуры

ОСНОВНЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ: 187-ФЗ

С 1 января 2018 года вступил в силу Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", который накладывает ряд обязанностей на организации и учреждения, являющиеся субъектами критической инфраструктуры (КИИ).

Закон **регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры** Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Криминализация неправомерного воздействия на КИИ РФ (ст. 274.1 УК)

.

Инженеры будущего

О безопасности критической информационной инфраструктуры

СУБЪЕКТЫ И ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Здравохранение 

Банковская сфера и иные сферы финансового рынка 

Топливно-энергитический комплекс 

Атомная промышленность 

Военно-промышленный комплекс 

Объекты КИИ

- информационные системы
- телекоммуникационные сети
- автоматизированные системы управления технологическими процессами

 Ракетно-космическая промышленность

 Горнодобывающая промышленность

 Металургическая и химическая промышленность

 Наука, транспорт, связь

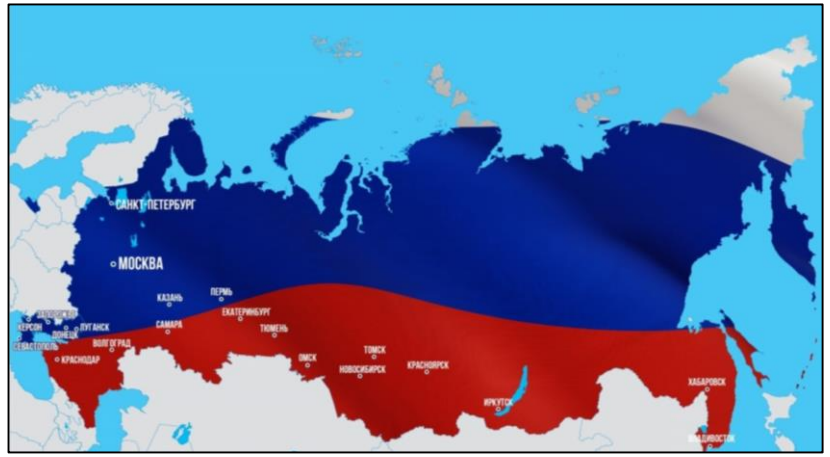
 Юр. лица и ИП, которые взаимодействуют с системами КИИ

КИБЕРБЕЗОПАСНОСТЬ: США и Россия

США

- Новые федеральные структуры
- Законы и нормативная база
- Единые квалификационные требования к кадрам
- Сотни стандартов
- Международные программы сертификации специалистов
- Лучшее в мире кибероружие

СИСТЕМА КИБЕРЗАЩИТЫ И КИБЕРНАПАДЕНИЯ



РОССИЯ

ТОЛЬКО СИСТЕМА КИБЕРЗАЩИТЫ

Безопасность начинается с тебя!

Человеческие факторы, способствующие росту атак на промышленные предприятия

- Устаревшие представления о кибербезопасности, ориентация на защиту периметра
- Повышение уровня доверия к автоматизированным системам
- Рост числа квалифицированных пользователей (возможностей персонала по обходу средств защиты)
- Рост квалификации и числа разработчиков, снижение стоимости атак
- Слабая подготовка персонала в целом в области информационной безопасности

Безопасность начинается с тебя!

Промышленность всё больше интересует хакеров
Особенно ТЭК и ОПК.

Атаки становятся все успешнее,
а сценарии — сложнее, последствия катастрофичнее.

Работа служб информационной безопасности
без помощи со стороны сотрудников просто невозможна

Культура информационной безопасности –
необходимая составная часть информационной защиты компании.

В России подготовлена серьезная нормативная база
по защите объектов критической информационной инфраструктуры:
187-ФЗ, приказы ФСТЭК, требования ФСБ и т.п.

Современные средства защиты
позволяют эффективно защищать в т.ч. от сложных атак на промышленные объекты и АСУ-ТП

Безопасность начинается с тебя!

- Не сохраняй имя пользователя и пароль в форме аутентификации удаленного доступа (например в браузере или RDP)
- Не использую неучтенные носители (флешек и т.п.)
- Не запускай посторонние программы на компьютере
- Не скачивай (и тем более не запускай!) программы из Интернет на корпоративные компьютеры
- Не открывай вложения в электронных письмах от неизвестного источника
- При звонках от неизвестных (другого отдела и т.п.) всегда проси подтвердить личность
- Не используй основной номер телефона для регистрации в программах лояльности, на сайтах и т.п. Заведи 2ю сим-карту!
- Не переходи по ссылкам из неизвестных источников
- Не отключай защитное ПО (антивирусы и т.п.)
- Не используй простые пароли, не храни их в текстовом виде
- Блокируй экран компьютер, покидая рабочее место

Инженеры будущего

СПАСИБО ЗА ВНИМАНИЕ !

Сергеев Антон Валерьевич

Советник, доцент МИЭМ НИУ ВШЭ

avsergeev@hse.ru

Семичаснов Илья Владимирович

Директор Центра управления
проектными разработками МИЭМ НИУ ВШЭ

isemichasnov@hse.ru