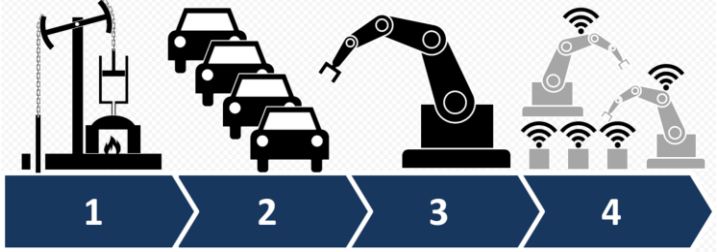
infotecs®

Тренды информационной безопасности

Докладчик: Алабина Юлия
alabinajf@infotecs.ru

Переход к новому технологическому укладу. Цифровая экономика



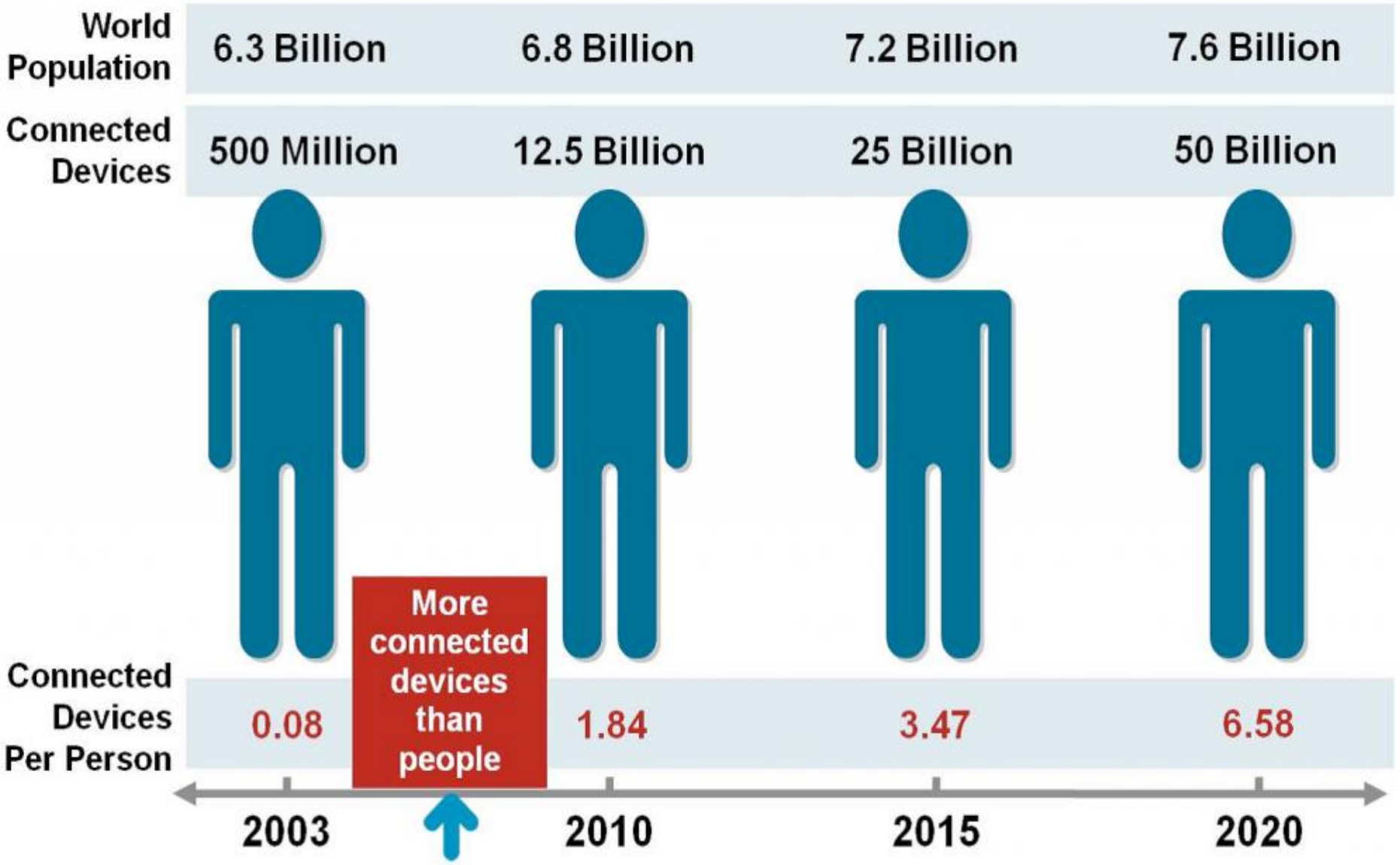
Этапы формирования цифровой экономики и рынков цифровой информации:

- Перевод накопленной аналоговой информации в цифровую и постепенный переход к созданию информации в цифровом виде
- Массовая генерация пользователями цифрового контента и формирование бизнес-процессов, построенных на предоставлении сервисов для производства, распространения и использования этой информации
- Генерация цифровой информации в результате взаимодействия «умных» устройств, формирование бизнес-процессов на основе Интернета вещей/ Промышленного интернета/ Киберфизических систем/ Киберсоциальных систем

Переход к новому технологическому укладу. Цифровая экономика

Источник: Cisco

Рост количества устройств IoT

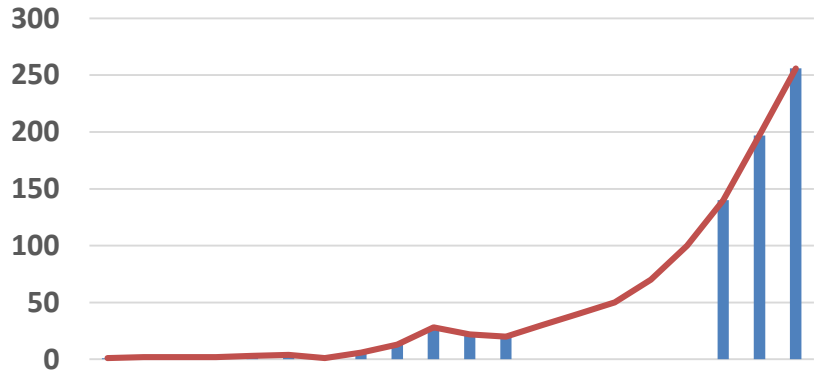


Киберфизические объекты и киберсистемы

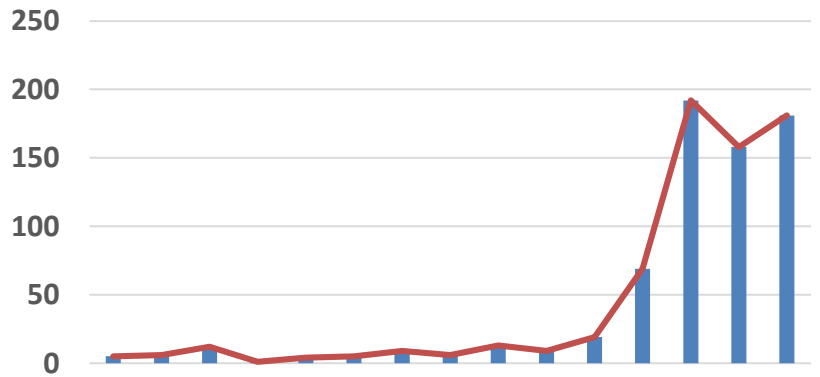
— Системы управления производством (АСУ ТП, SCADA-системы).
— Интернет вещей (Internet of Things, умный дом, умные вещи).
— Робото-технические системы критического назначения.
— Беспилотные летательные аппараты и беспилотные автомобили.
— Системы военного назначения и др.

Статистика нарушений безопасности

Количество инцидентов безопасности



Количество уязвимостей компонентов АСУ ТП



Наиболее серьезным фактором, вызвавшим рост количества проблем обеспечения безопасности в системах АСУ ТП, явилась тенденция к интеграции их с традиционными (корпоративными) ИТ-системами

Инциденты нарушения безопасности киберфизических систем

Нефтяная компания Saudi Aramco

- Крупнейшая нефтяная компания в мире Saudi Aramco стала жертвой направленной атаки на свои офисы. Хакеры получили доступ к сети благодаря атаке на одного из сотрудников компании, через которого смогли получить доступ к 30 000 компьютеров в сети. В какой-то момент хакерам удалось удалить содержимое всех компьютеров, в то время как на экранах показывался горящий американский флаг.

Департамент автомобильных дорог и транспорта в США

- Были заражены 200 компьютеров Департамента автомобильных дорог и транспорта в округе Кук (штат Иллинойс). Эти системы отвечали за поддержание сотни километров дорог в пригороде Чикаго. В результате атаки пришлось отключать сеть на 9 дней, чтобы вылечить все компьютеры.

Металлургический завод в Германии

- Используя социальную инженерию, хакеры сумели получить доступ к компьютеру одного сотрудника, с которого они смогли получить доступ к внутренней сети системы управления. В результате этого стало невозможным выключить одну из домен, что нанесло огромный ущерб предприятию.

Система управления температурой воды и отоплением в Финляндии

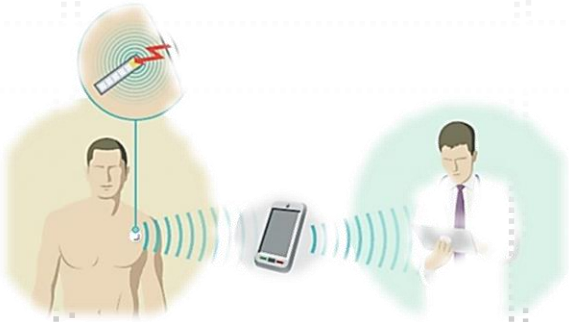
- Жители многоквартирных домов в финском городе Лаппеэнранта провели неделю без отопления и горячей воды. Причиной стала мощная DDoS-атака на "умную" систему контроля температуры воды и давления в батареях отопления.

Интернет вещей. Угрозы

Атаки на бытовые устройства

Атаки на транспортные сети

Атаки на сети медицинского назначения

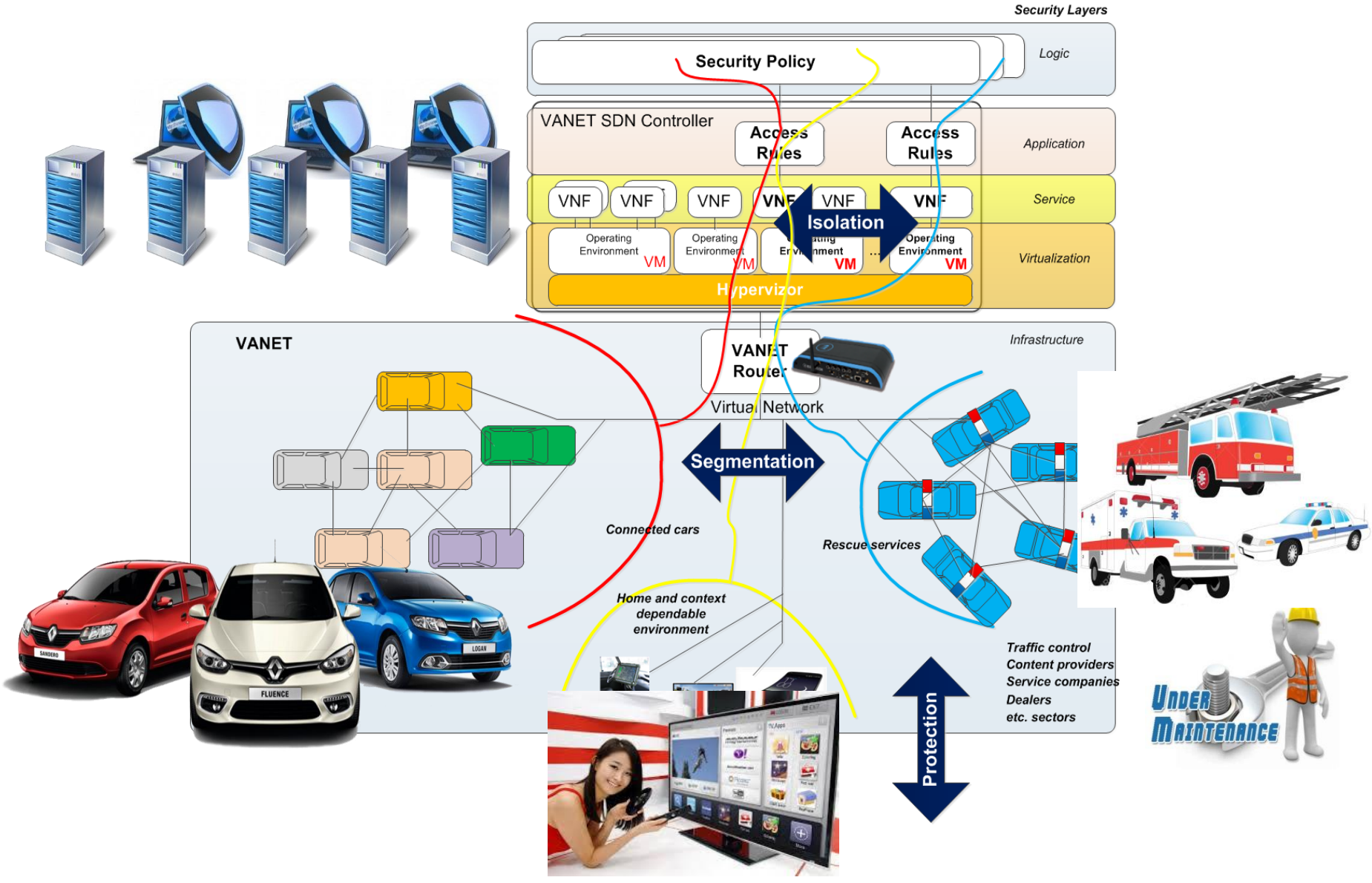


Атаки на СМИ

Дезинформация, информационно-психологическое воздействие

Нанесение вреда жизни и здоровью людей

Беспилотный транспорт и Интернет вещей. Новые угрозы



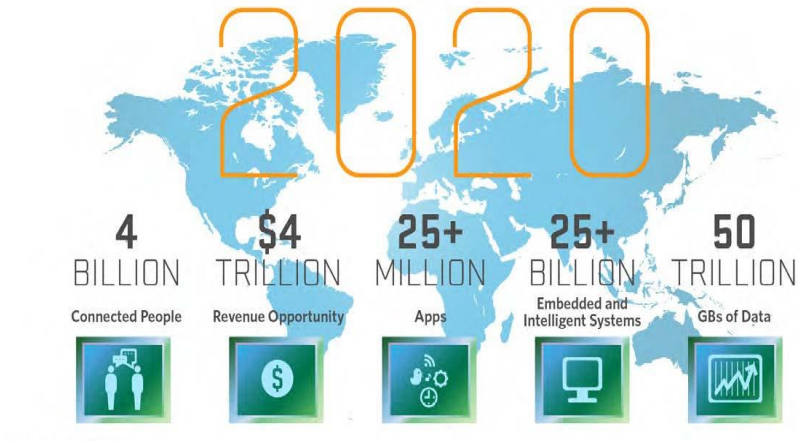
ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ИНТЕРНЕТЕ ВЕЩЕЙ

«Обратная связь» Интернет-вещей с их владельцами и пользователями

- Интернет-вещи получают реальную информацию от своего владельца или пользователя
- Данные, всесторонне характеризующие владельца или пользователя, поступают в Интернет без помощи человека
- Информация о каждом пользователе «умных» устройств уже находится в Интернете
- Компании, способные обрабатывать и анализировать большие объемы данных, знают о пользователе больше информации, чем он хотел бы им предоставить

Непроизвольная утрата неприкосновенности частной жизни пользователями «умных» устройств

Текущее состояние защищенности Интернета вещей от киберугроз

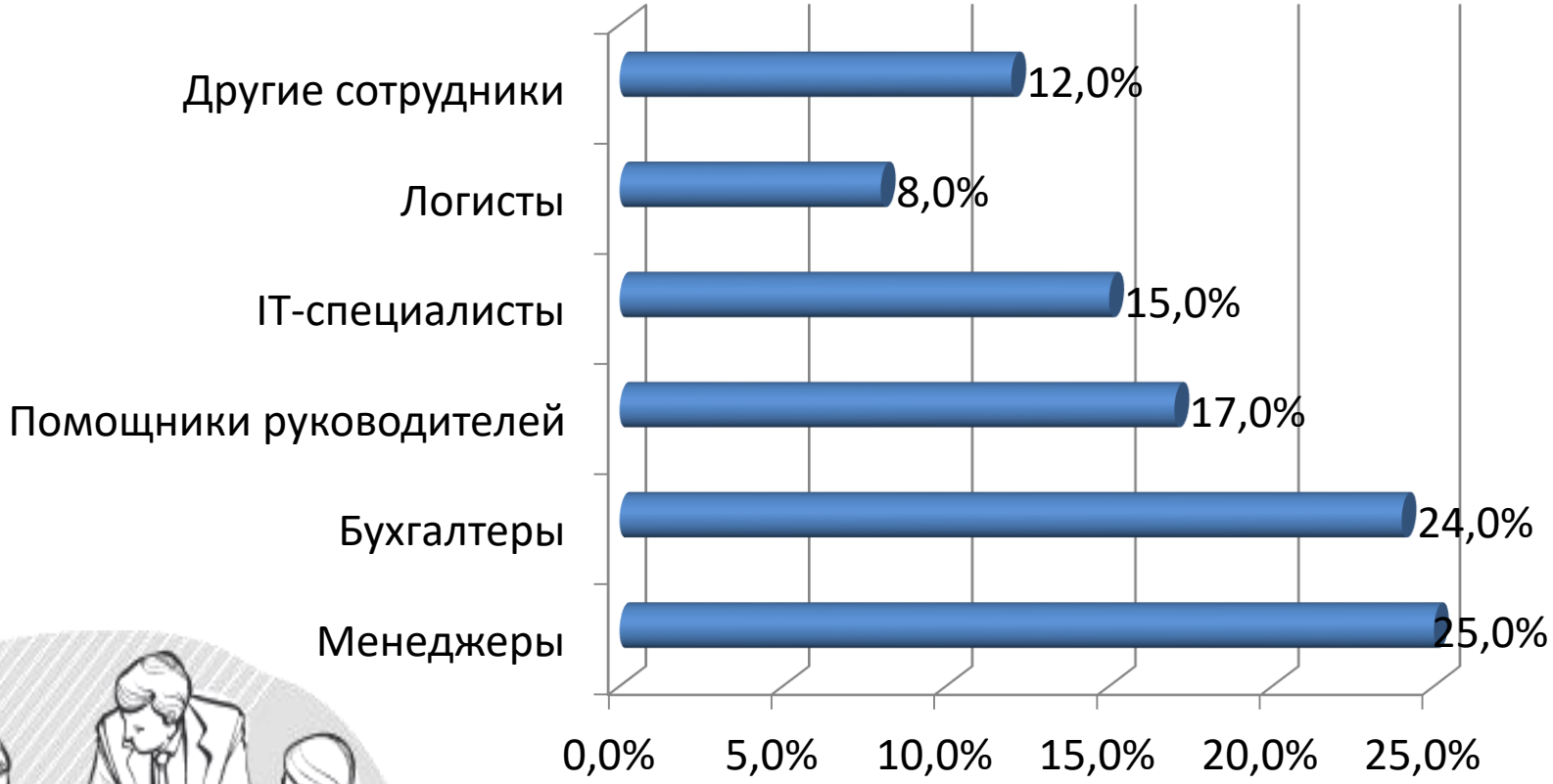


По результатам исследований HP:

- **62%** устройств обладают уязвимым веб-интерфейсом
- **71%** наиболее часто используемых «умных» приборов, имеющих выход в сеть, уязвимы
- **85%** устройств подвержены утечке информации в той или иной степени и когда-то «выдавали» личную информацию о своих владельцах
- **90%** устройств собирают ту или иную персональную информацию о владельце без его ведома

Атаки не на «компьютерные» системы, а на «реальные» (кардиостимуляторы, бытовые устройства, автотранспорт и т.д.)

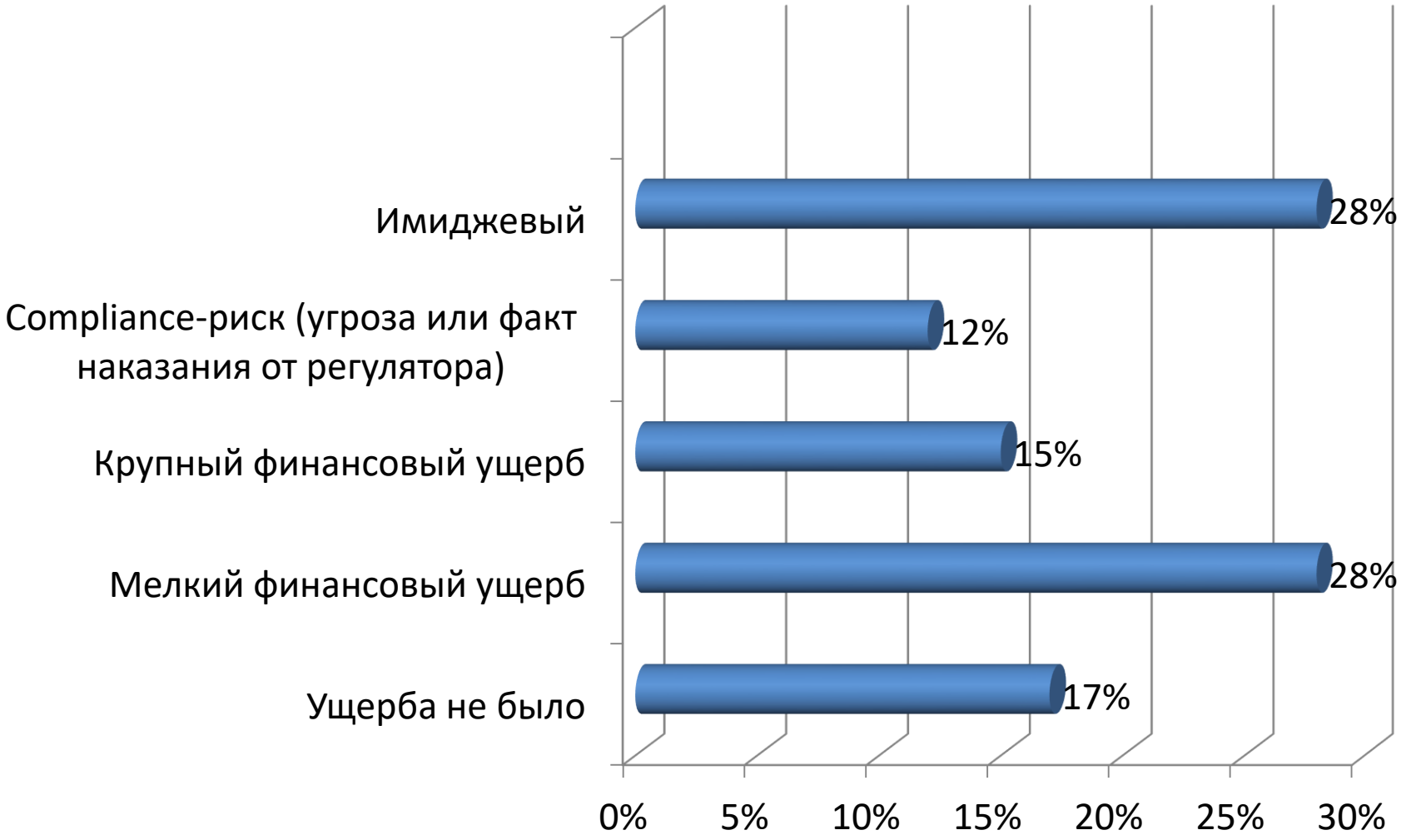
Статистика нарушений безопасности внутри организации



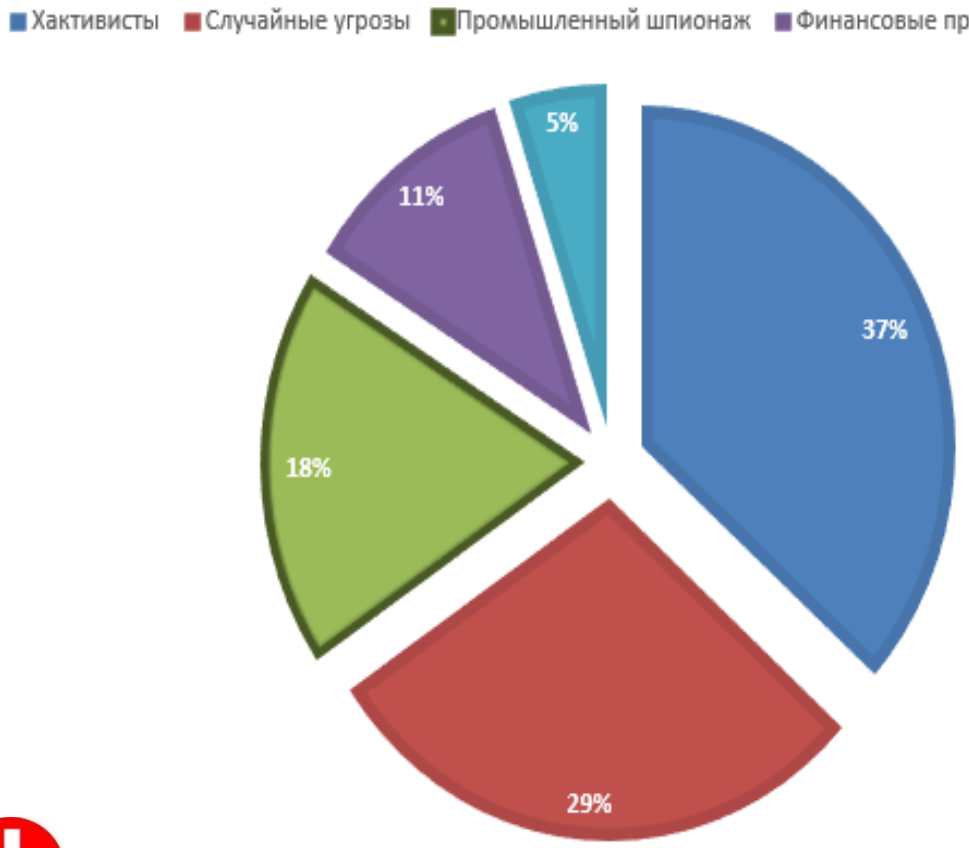
Увеличилась доля утечек по сетевому каналу и электронной почте.

Снизились доли утечек в результате кражи/потери оборудования, через съемные носители и бумажные документы.

Ущерб от инцидентов



Источники угроз ИБ КИИ
Доля участия и влияния киберподразделений



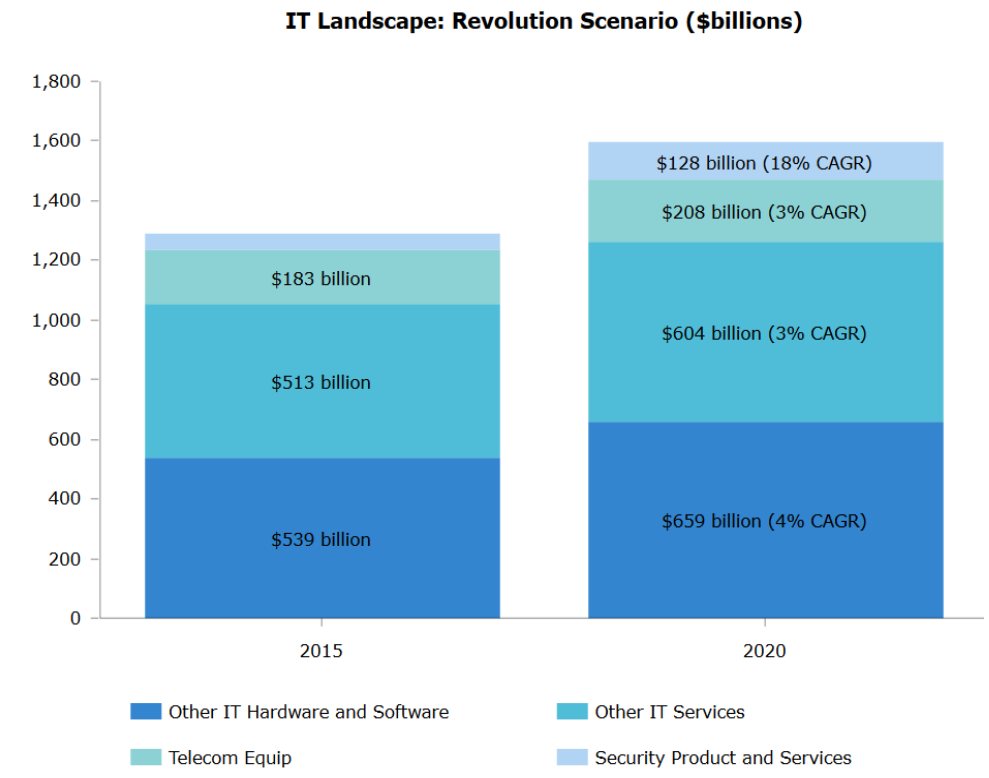
Около 20% серьезных инцидентов было организовано группами промышленного шпионажа или военных киберподразделений

Рынок информационной безопасности

Сохраняется рост

- Общемировой тренд

Cybersecurity Market Could Grow by More Than Four Times Overall IT Spend



Объем рынка продуктов и услуг кибербезопасности превысил 60 млрд. $ США в 2018 году, и эта цифра удвоится к концу 2020 году.

Рынок информационной безопасности

Рост обусловлен

- Цифровой экономикой
  - Резкому расширению компьютерной взаимозависимости и экспоненциальному увеличению потоков данных и вычислительной мощности государственных и корпоративных сетей
  - Проникновению цифровых коммуникаций в новые области
- Изменениями в существующих подходах и технологиях кибербезопасности и появлению новых технологий и подходов атак
- Изменениями оценок критериев рисков
- Сегментацией глобального рынка на изолированные суверенные сегменты
- За счет роста стоимости кибербезопасности

Рынок сервисов ИБ будет расти с 17,02 млрд. долл. США в 2016 году, до 33,68 млрд. долл. США к 2021 году, при совокупном годовом темпе роста (CAGR) в 14,6% с 2016 года по 2021 год

- Managed Intrusion Detection Prevention System
- Unified Threat Management
- Vulnerability Management
- Compliance Management
- Managed Security Information And Event Management
- Identity And Access Management
- Antivirus/Antimalware
- Web Sec and Others

Средства кибербезопасности

infotecs®

Комплексное решение по защите

Сетевая платформа в составе:

Межсетевой экран

Сетевой экран приложений - DPI

VPN

Система предотвращения вторжений

Шлюзовой антивирус

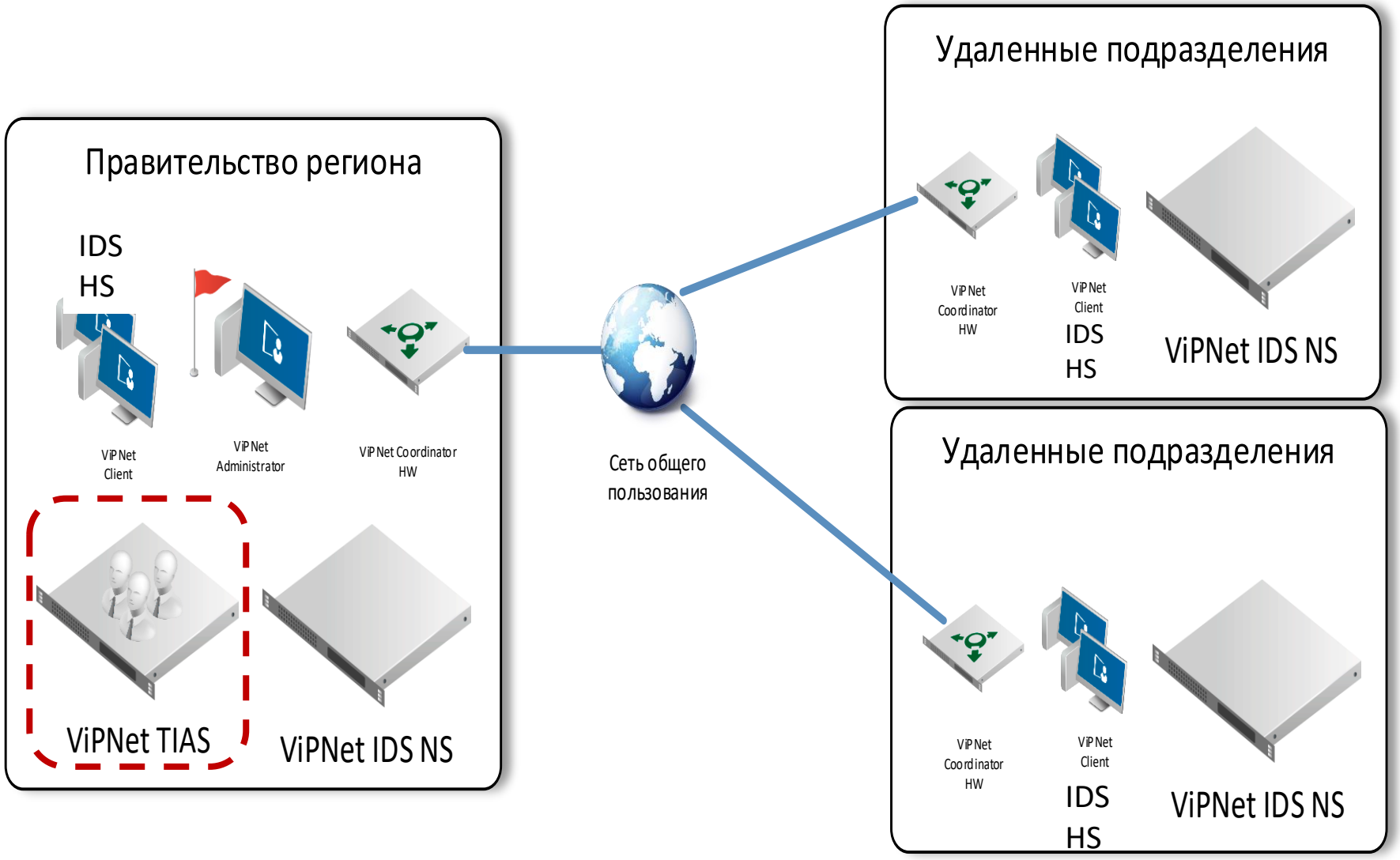
Интеграция с Active Directory

и т.д.


Завод
VPNet Coordinator HW
VPNet Coordinator IG
VPNet SIES
VPNet TLS Gateway
Заводоуправление
VPNet Coordinator HW
VPNet Client
VPNet IDS
VPNet IDS HS
VPNet TLS Gateway
VPNet PKI Client
VPNet TIAS
Офис
VPNet StateWatcher
VPNet Coordinator HW
VPNet Client
VPNet IDS HS
VPNet IDS
VPNet PKI Client
VPNet Connect
VPNet TIAS
VPNet Administrator
VPNet Policy Manager
Банк
VPNet HSM
VPNet PKI Client
VPNet TLS Gateway
VPNet IDS HS
VPNet IDS
VPNet Coordinator HW
VPNet TIAS
ЦОД / РЦОД
VPNet Coordinator HW/VA
VPNet IDS
Портал
VPNet TLS Gateway
VPNet HSM
VPNet Registration Point
VPNet Publication Service
http://
X: 184,06 cm
Y: 119,95 cm
Госуслуги
VPNet Connect
VPNet Client
VPNet Coordinator HW
VPNet PKI Client
VPNet EDI
Электроэнергетика
VPNet SIES
VPNet Coordinator IG
Железная дорога
VPNet Coordinator IG
VPNet Client
VPNet SIES
VPNet TIAS
Парк
VPNet Connect
VPNet Client
Поликлиника
VPNet PKI Client
VPNet TLS Gateway
VPNet IDS HS
VPNet IDS
VPNet Coordinator HW
VPNet Client
УЦ
VPNet Certification Authority
VPNet Coordinator HW
VPNet TLS Gateway
VPNet TSP OCSP
VPNet Registration Point
VPNet CA WEB
VPNet CA Informing

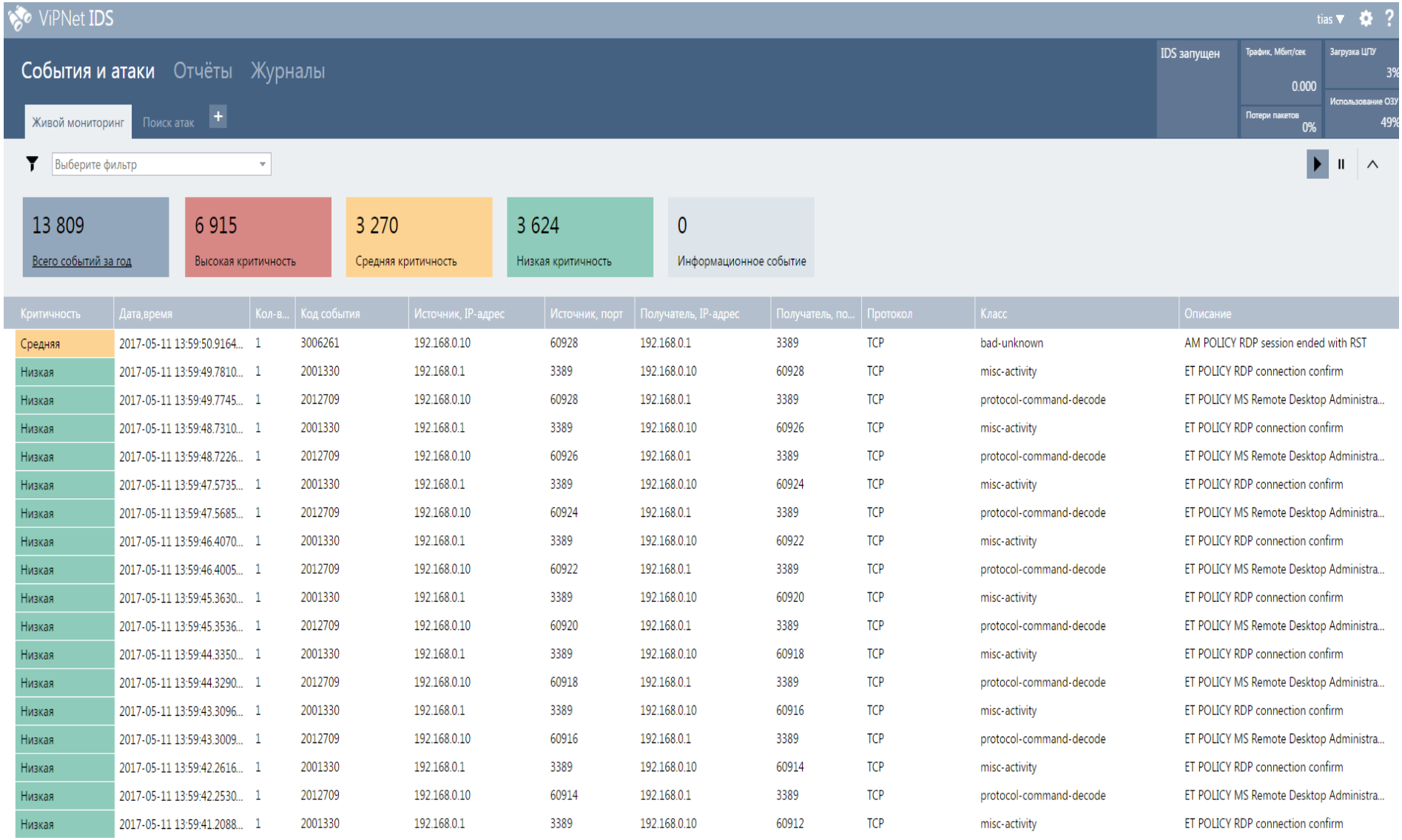
Интеллектуальная аналитическая система ViPNet TIAS

Пример использования TIAS



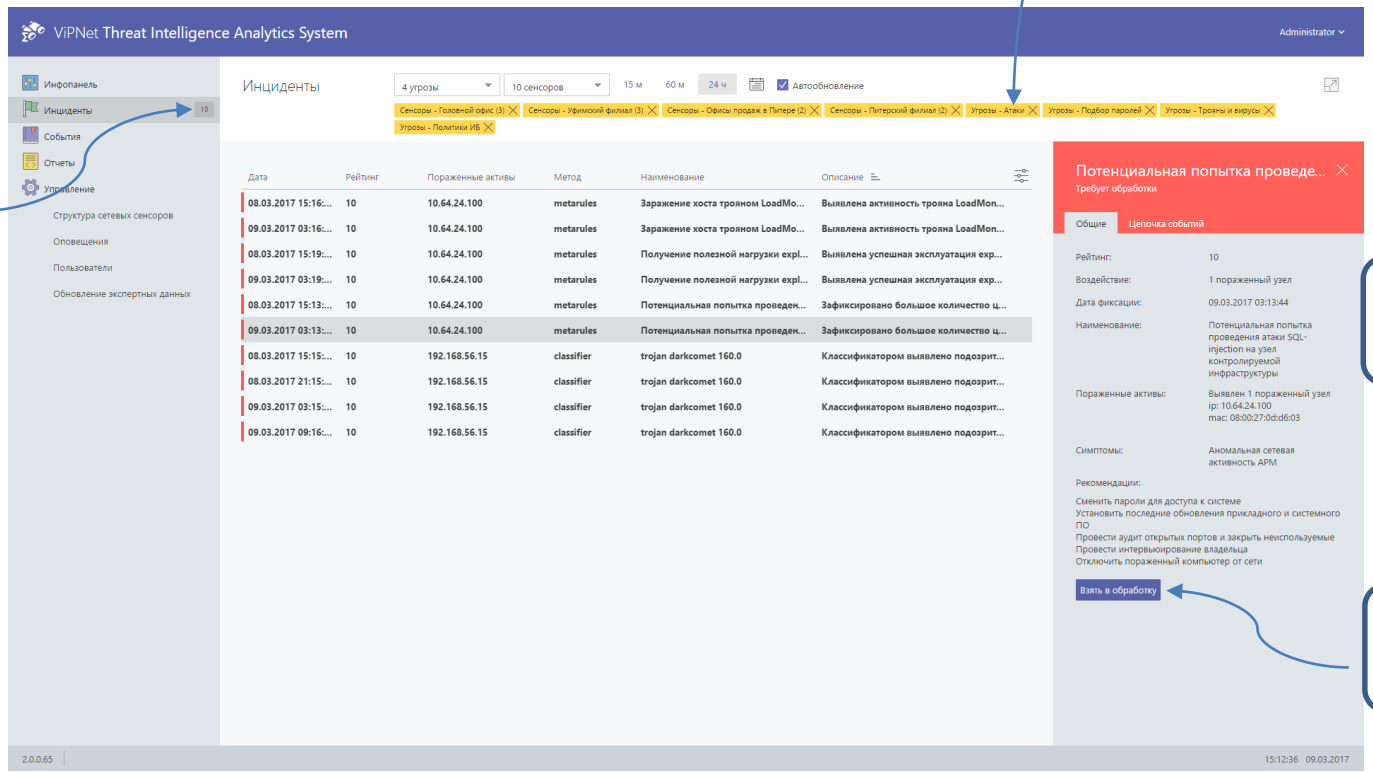
Экспертиза в области ИБ

Работа с IDS

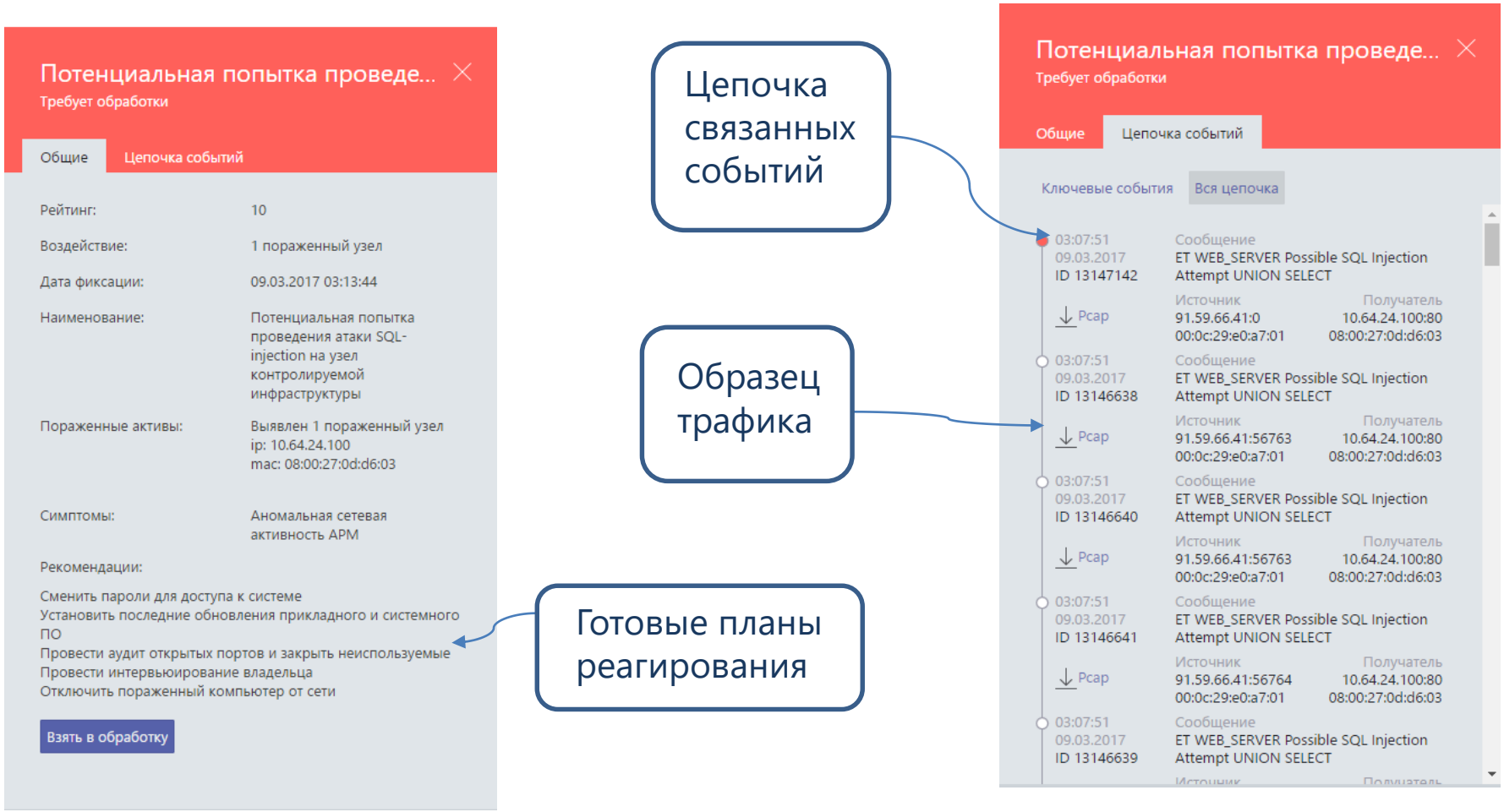


Критичность	Дата,время	Кол-в...	Код события	Источник, IP-адрес	Источник, порт	Получатель, IP-адрес	Получатель, по...	Протокол	Класс	Описание
Средняя	2017-05-11 13:59:50.9164...	1	3006261	192.168.0.10	60928	192.168.0.1	3389	TCP	bad-unknown	AM POLICY RDP session ended with RST
Низкая	2017-05-11 13:59:49.7810...	1	2001330	192.168.0.1	3389	192.168.0.10	60928	TCP	misc-activity	ET POLICY RDP connection confirm
Низкая	2017-05-11 13:59:49.7745...	1	2012709	192.168.0.10	60928	192.168.0.1	3389	TCP	protocol-command-decode	ET POLICY MS Remote Desktop Administra...
Низкая	2017-05-11 13:59:48.7310...	1	2001330	192.168.0.1	3389	192.168.0.10	60926	TCP	misc-activity	ET POLICY RDP connection confirm
Низкая	2017-05-11 13:59:48.7226...	1	2012709	192.168.0.10	60926	192.168.0.1	3389	TCP	protocol-command-decode	ET POLICY MS Remote Desktop Administra...
Низкая	2017-05-11 13:59:47.5735...	1	2001330	192.168.0.1	3389	192.168.0.10	60924	TCP	misc-activity	ET POLICY RDP connection confirm
Низкая	2017-05-11 13:59:47.5685...	1	2012709	192.168.0.10	60924	192.168.0.1	3389	TCP	protocol-command-decode	ET POLICY MS Remote Desktop Administra...
Низкая	2017-05-11 13:59:46.4070...	1	2001330	192.168.0.1	3389	192.168.0.10	60922	TCP	misc-activity	ET POLICY RDP connection confirm
Низкая	2017-05-11 13:59:46.4005...	1	2012709	192.168.0.10	60922	192.168.0.1	3389	TCP	protocol-command-decode	ET POLICY MS Remote Desktop Administra...
Низкая	2017-05-11 13:59:45.3630...	1	2001330	192.168.0.1	3389	192.168.0.10	60920	TCP	misc-activity	ET POLICY RDP connection confirm
Низкая	2017-05-11 13:59:45.3536...	1	2012709	192.168.0.10	60920	192.168.0.1	3389	TCP	protocol-command-decode	ET POLICY MS Remote Desktop Administra...
Низкая	2017-05-11 13:59:44.3350...	1	2001330	192.168.0.1	3389	192.168.0.10	60918	TCP	misc-activity	ET POLICY RDP connection confirm
Низкая	2017-05-11 13:59:44.3290...	1	2012709	192.168.0.10	60918	192.168.0.1	3389	TCP	protocol-command-decode	ET POLICY MS Remote Desktop Administra...
Низкая	2017-05-11 13:59:43.3096...	1	2001330	192.168.0.1	3389	192.168.0.10	60916	TCP	misc-activity	ET POLICY RDP connection confirm
Низкая	2017-05-11 13:59:43.3009...	1	2012709	192.168.0.10	60916	192.168.0.1	3389	TCP	protocol-command-decode	ET POLICY MS Remote Desktop Administra...
Низкая	2017-05-11 13:59:42.2616...	1	2001330	192.168.0.1	3389	192.168.0.10	60914	TCP	misc-activity	ET POLICY RDP connection confirm
Низкая	2017-05-11 13:59:42.2530...	1	2012709	192.168.0.10	60914	192.168.0.1	3389	TCP	protocol-command-decode	ET POLICY MS Remote Desktop Administra...
Низкая	2017-05-11 13:59:41.2088...	1	2001330	192.168.0.1	3389	192.168.0.10	60912	TCP	misc-activity	ET POLICY RDP connection confirm

Инциденты


Заданные фильтры
Новые инциденты
Описание инцидента
Взять в обработку
ViPNet Threat Intelligence Analytics System
Administrator
Инфопанель
Инциденты
События
Отчеты
Управление
Структура сетевых сенсоров
Оповещения
Пользователи
Обновление экспертных данных
Инциденты
4 угрозы
10 сенсоров
15 м
60 м
24 ч
Автообновление
Сенсоры - Головной офис (3)
Сенсоры - Уфимский филиал (3)
Сенсоры - Офисы продаж в Питере (2)
Сенсоры - Питерский филиал (2)
Угрозы - Атаки
Угрозы - Подбор паролей
Угрозы - Трояны и вирусы
Угрозы - Политики ИБ
Дата
Рейтинг
Пораженные активы
Метод
Наименование
Описание
08.03.2017 15:16:... 10 10.64.24.100 metarules Заражение хоста трояном LoadMo... Выявлена активность трояна LoadMon...
09.03.2017 03:16:... 10 10.64.24.100 metarules Заражение хоста трояном LoadMo... Выявлена активность трояна LoadMon...
08.03.2017 15:19:... 10 10.64.24.100 metarules Получение полезной нагрузки expl... Выявлена успешная эксплуатация exp...
09.03.2017 03:19:... 10 10.64.24.100 metarules Получение полезной нагрузки expl... Выявлена успешная эксплуатация exp...
08.03.2017 15:13:... 10 10.64.24.100 metarules Потенциальная попытка проведен... Зафиксировано большое количество ц...
09.03.2017 03:13:... 10 10.64.24.100 metarules Потенциальная попытка проведен... Зафиксировано большое количество ц...
08.03.2017 15:15:... 10 192.168.56.15 classifier trojan darkcomet 160.0 Классификатором выявлено подозрит...
08.03.2017 21:15:... 10 192.168.56.15 classifier trojan darkcomet 160.0 Классификатором выявлено подозрит...
09.03.2017 03:15:... 10 192.168.56.15 classifier trojan darkcomet 160.0 Классификатором выявлено подозрит...
09.03.2017 09:16:... 10 192.168.56.15 classifier trojan darkcomet 160.0 Классификатором выявлено подозрит...
Потенциальная попытка проведе...
Требует обработки
Общие
Цепочка событий
Рейтинг: 10
Воздействие: 1 пораженный узел
Дата фиксации: 09.03.2017 03:13:44
Наименование: Потенциальная попытка проведения атаки SQL-injection на узел контролируемой инфраструктуры
Пораженные активы: Выявлен 1 пораженный узел ip: 10.64.24.100 mac: 08:00:27:0d:d6:03
Симптомы: Аномальная сетевая активность АРМ
Рекомендации:
Сменить пароли для доступа к системе
Установить последние обновления прикладного и системного ПО
Провести аудит открытых портов и закрыть неиспользуемые
Провести интервьюирование владельца
Отключить пораженный компьютер от сети
Взять в обработку
2.0.0.65
15:12:36 09.03.2017

Карточка инцидента

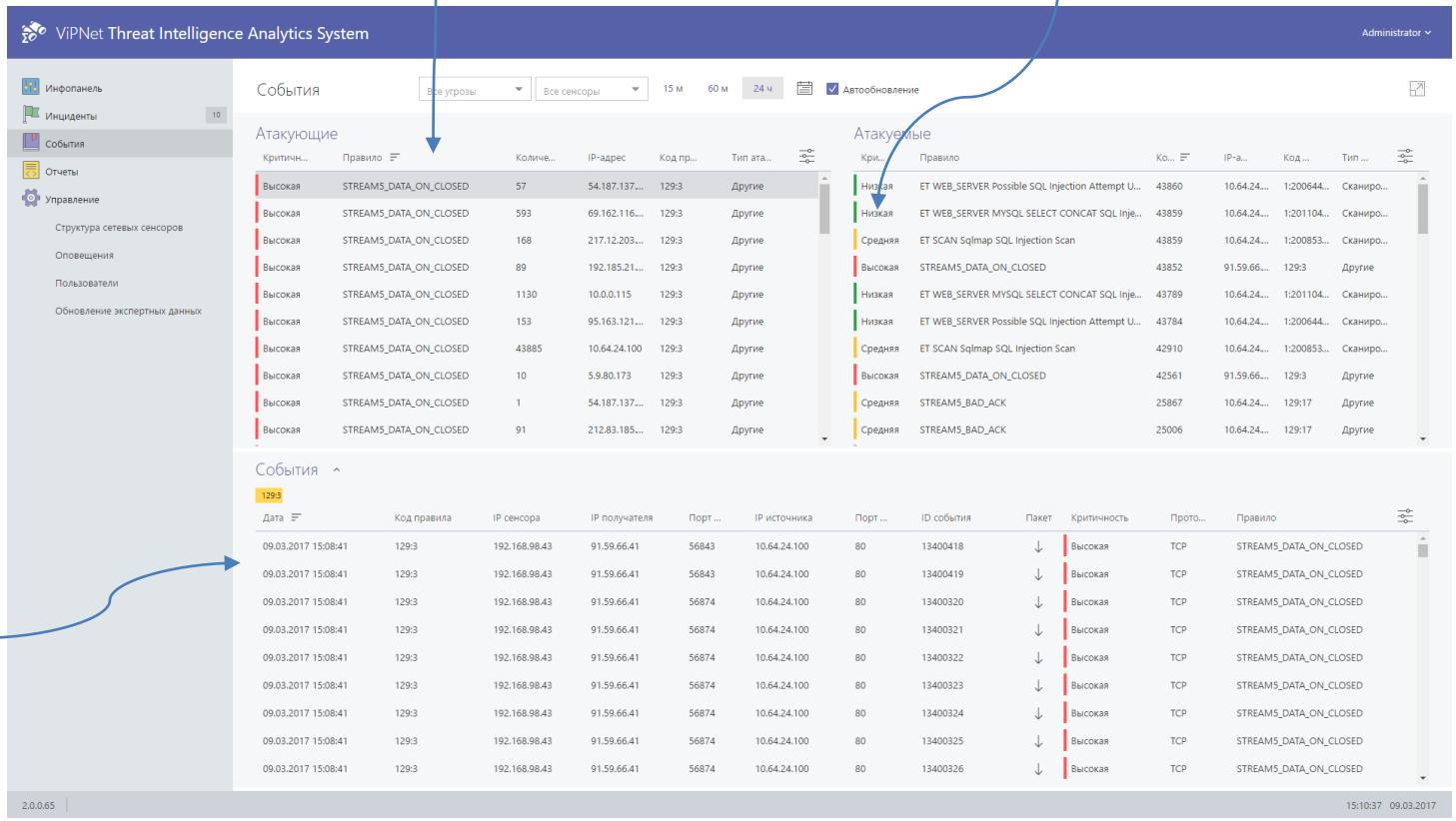


События

Группы событий

Критичность события

Все события выбранной группы

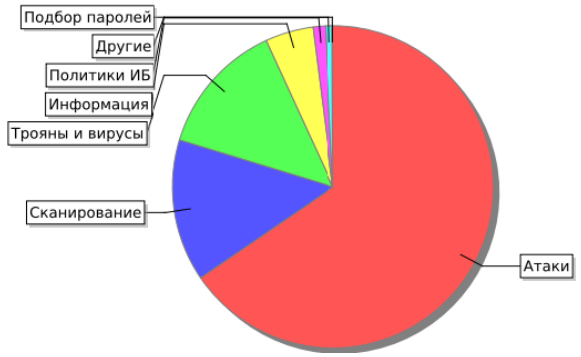


Статистика и отчетность

Статистика по событиям
Распределение событий по категориям

События с 9/15/16 4:50 PM по 9/16/16 3:57 PM

Наименование	Количество
Атаки	28008
Сканирование	6097
Трояны и вирусы	5745
Информация	2071
Политики ИБ	537
Другие	314
Подбор паролей	14



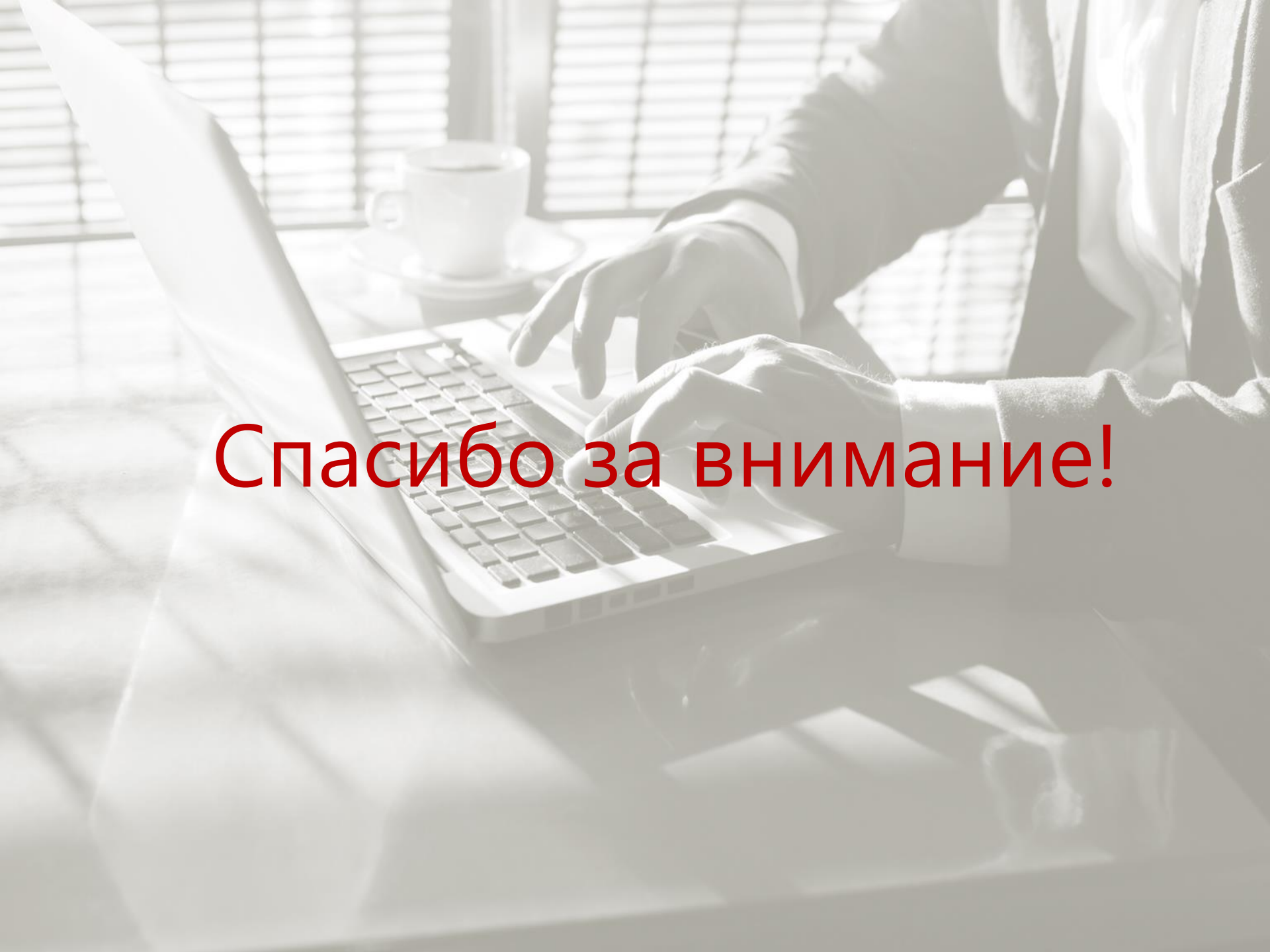
Статистика по инцидентам
Инциденты ИБ

События с 2/20/17 12:16 PM по 2/21/17 12:16 PM

Наименование	Время обнаружения
Получение полезной нагрузки exploit kit Angler узлом контролируемой сети	2/21/17 7:58 AM
trojan darkcomet 160.0	2/21/17 7:53 AM
Потенциальная попытка проведения атаки SQL-injection на узел контролируемой инфраструктуры	2/21/17 7:51 AM
Заражение хоста трояном LoadMoney	2/21/17 7:51 AM
trojan darkcomet 160.0	2/21/17 1:52 AM
Активность бота спамера	2/21/17 1:20 AM
Получение полезной нагрузки exploit kit Angler узлом контролируемой сети	2/20/17 7:57 PM
trojan darkcomet 160.0	2/20/17 7:52 PM
Потенциальная попытка проведения атаки SQL-injection на узел контролируемой инфраструктуры	2/20/17 7:50 PM
Заражение хоста трояном LoadMoney	2/20/17 7:50 PM
trojan darkcomet 160.0	2/20/17 1:52 PM
Активность бота спамера	2/20/17 1:20 PM

В заключение:

- ✓ Источники угроз – квалифицированные, высокоорганизованные группы злоумышленников
- ✓ Максимальная угроза – инфраструктурные объекты и объекты КИИ
- ✓ Фокус при защите на системы управления и комплексный подход
- ✓ Специалисты по кибербезопасности очень востребованы на рынке



Спасибо за внимание!