innopolis university

Вопросы реализации требований по КИИ

Петренко Сергей Анатольевич
руководитель Центра ИБ,
Профессор, д.т.н.

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

Цифровая трансформация бизнеса ускоряется

Умный город

Банк 3.0

Умный транспорт

Умные электросети

Умное производство

Умное образование

Новые интернет-провайдеры

ТЕХНОЛОГИИ ИНДУСТРИИ 4.0

Решение Huawei IoT и Big Data

Приложения

Мониторинг подвижного состава

Мониторинг оборудования вдоль ж/д полотна

Мониторинг систем электропитания

Мониторинг окружающей обстановки, сбор данных

Платформа IoT

Богатство приложений

Открытые API для партнеров

Различные сервисы и услуги

Удобное управление

“Всегда на связи”

Безопасность / Идентификация

Большие Данные

1-на платформа (аппаратно-программный комплекс)

Сеть доступа

Беспроводная сеть (eLTE / NB-IoT и др.)

Сеть IP

Маршрутизатор IoT

Интеграционный модуль IoT

Шлюз IoT

2 типа доступа (проводной и беспроводной)

Терминалы

Операционная система Lite OS

Подвижной состав

Железнодорожные пути

Депо / станция

1-на операционная система (Lite OS)

АКТУАЛЬНОСТЬ ТЕМЫ. КЛЮЧЕВОЕ НАПРАВЛЕНИЕ ГОСПРОГРАММЫ «ЦИФРОВАЯ ЭКОНОМИКА» РФ

Innopolis University

Единые сети устройств

Дополненная реальность

Интернет вещей

Машинное обучение

«Умные» автомобили

Искусственный интеллект

Сервисы в дополненной реальности

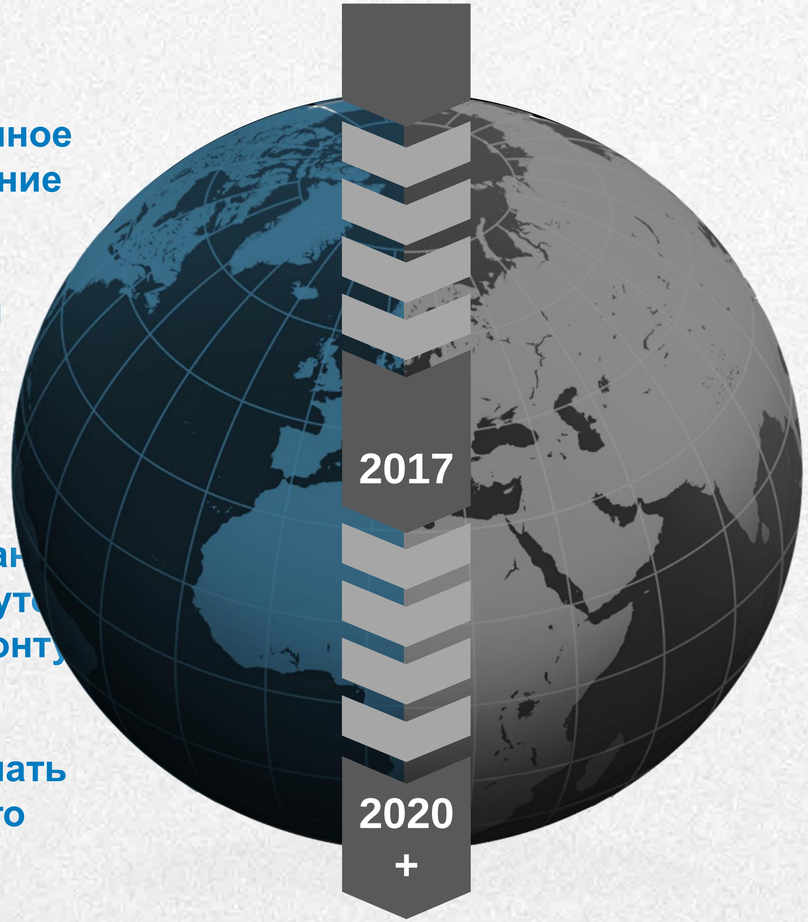
Компан
Замкнут
Инфо конт

Импланты

3D печать всего

«Умные» андроиды

Единое информационное поле



DDoS-атаки любой мощности

Кража биометрии

Атаки по индустриальной сети

Покушения через умный транспорт

Сложные APT атаки

Умные бот сети

Открытая продажа информации

Кража личности

Прямые атаки на здоровье

Отключение целых компаний

Подделка драгметаллов

Восстание машин

ПРОСТО РЕАГИРОВАНИЯ УЖЕ НЕ ДОСТАТОЧНО

INNOPOLIS UNIVERSITY

«Генералы всегда готовятся к прошлой войне…»
- У. Ч

Цель: обеспечить защиту

Непрерывность ИТ, защита от аварий
- Скачки электроэнергии
- Отказ оборудования
- Утечка по каналам ПЭМИН

«человеко-центричность»

Information Security
- Вирусные инциденты
- Подделка электронных документов
- DDoS-атаки

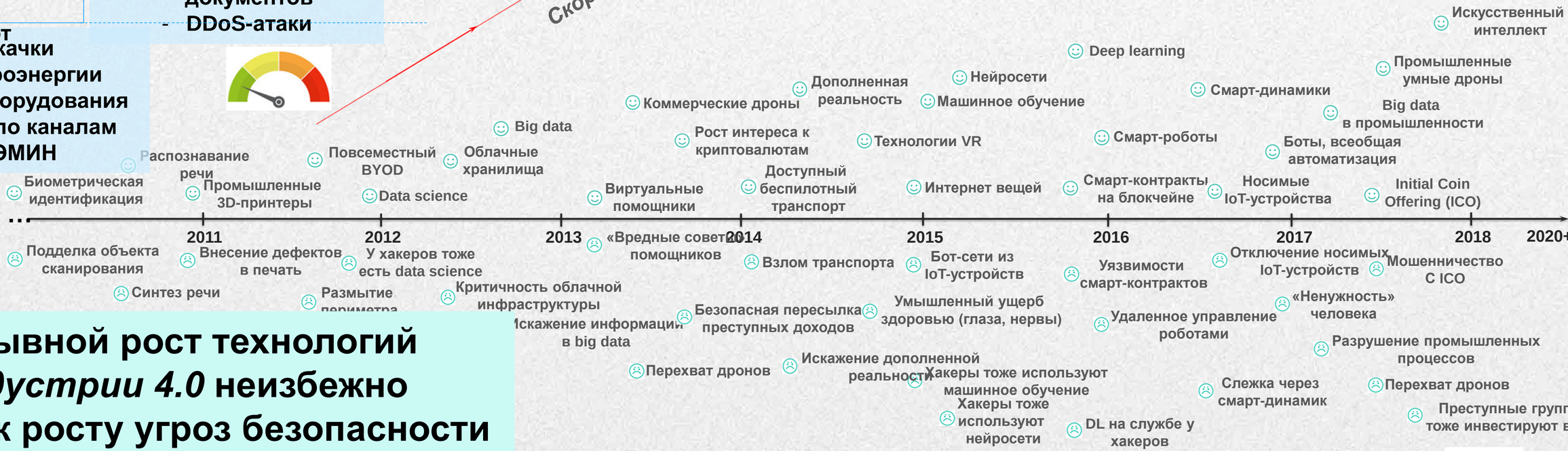
Цель: обнаружить как можно раньше, минимизировать последствия

Cyber Security
- APT-атаки
- «Кража личности»
- Недоступность данных, хранящихся в облаке

Cyber Resilience
- Кибероружие
- Атаки на АСУ ТП
- Сложные вирусные эпидемии

Скорость появления новых киберугроз

Актуальна именно
Киберустойчивость
– как ответ на скорость появления новых технологий и рост угроз безопасности



Взрывной рост технологий *Индустрии 4.0* неизбежно привел к росту угроз безопасности

5

Беспрецедентный рост угроз безопасности

INNOPOLIS UNIVERSITY

2016

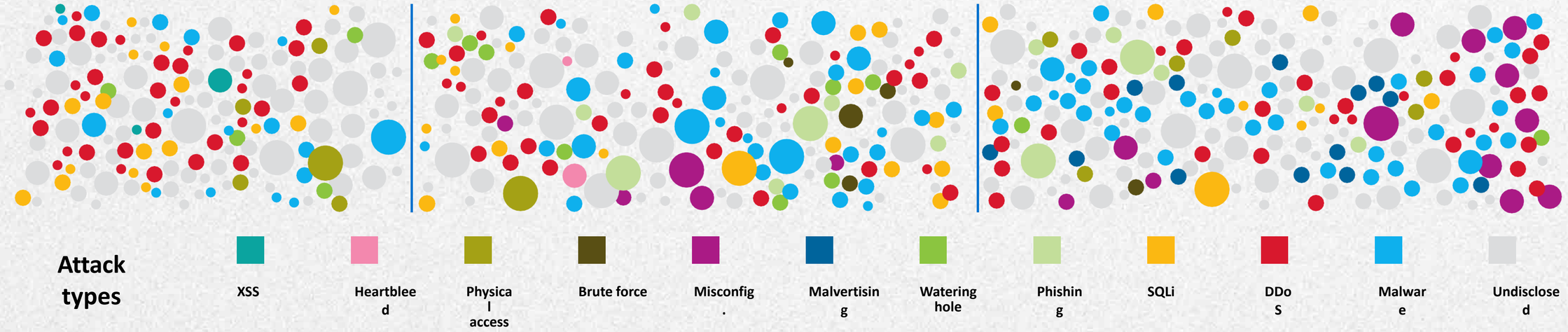
800+ млн случаев атак

2018

71+ млрд случаев атак

2019

Беспрецедентное количество сочетанных атак



256 дней

среднее время на выявление целевой атаки

2 трлн $

оценка рынка киберпреступности в 2019

Требования к системам безопасности значимых объектов КИИ (Приказ ФСТЭК России от 21 декабря 2017 г. № 235)

Программные и программно-аппаратные средства, применяемые для обеспечения безопасности значимых объектов КИИ :

- **СЗИ, в том числе СЗИ от НСД (включая встроенные в общесистемное, прикладное программное обеспечение)**
- **межсетевые экраны**
- **средства обнаружения (предотвращения) вторжений (компьютерных атак)**
- **средства антивирусной защиты**
- **средства (системы) контроля (анализа) защищенности**
- **средства управления событиями безопасности**
- **средства защиты каналов передачи данных**

Требования к системам безопасности значимых объектов КИИ (Приказ ФСТЭК России от 21 декабря 2017 г. № 235)

Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ:

- средства должны пройти оценку соответствия
- в случае, если объектом КИИ обрабатывается государственная тайна или объект КИИ представляет собой государственную информационную систему, сертификация обязательна
- в приоритетном порядке применяются встроенные в рабочие системы специальные программные СЗИ
- СЗИ должны применяться в соответствии с эксплуатационной документацией и обязательно сопровождаться поддержкой со стороны разработчика
- При создании системы также должны учитываться возможные ограничения самого разработчика, например, запрет использования средства на определённых объектах
- порядок применения СЗИ определяется субъектом КИИ в организационно-распорядительных документах по безопасности значимых объектов с учетом особенностей деятельности субъекта КИИ

Организационные и технические меры в значимых объектах КИИ (Приказ ФСТЭК России от 25 декабря 2017 г. № 239)

- идентификация и аутентификация (ИАФ)
- управление доступом (УПД)
- ограничение программной среды (ОПС)
- защита машинных носителей информации (ЗНИ)
- аудит безопасности (АУД)
- антивирусная защита (АВЗ)
- предотвращение вторжений (компьютерных атак) (СОВ)
- обеспечение целостности (ОЦЛ)
- обеспечение доступности (ОДТ)
- защита технических средств и систем (ЗТС)
- защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
- планирование мероприятий по обеспечению безопасности (ПЛН)
- управление конфигурацией (УКФ)
- управление обновлениями программного обеспечения (ОПО)
- реагирование на инциденты информационной безопасности (ИНЦ)
- обеспечение действий в нештатных ситуациях (ДНС)
- информирование и обучение персонала (ИПО)

Состав мер в зависимости от категории значимости приведен в приложении к «Требованиям…» (приказ ФСТЭК России от 25 декабря 2017 г. № 239)

Применение СЗИ в значимых объектах КИИ (Приказ ФСТЭК России от 25 декабря 2017 г. № 239)

В случае использования в значимом объекте сертифицированных на соответствие требованиям по безопасности информации СЗИ:

- **в значимых объектах 1 категории применяются СЗИ не ниже 4 класса защиты**
- **в значимых объектах 2 категории применяются СЗИ не ниже 5 класса защиты**
- **в значимых объектах 3 категории применяются СЗИ 6 класса защиты**

При этом в значимых объектах 1 и 2 категорий значимости применяются сертифицированные СЗИ, прошедшие проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

Субъектом критической информационной инфраструктуры может быть принято решение о повышении уровня контроля отсутствия недекларированных возможностей средств защиты информации

Применение СЗИ в значимых объектах КИИ (Приказ ФСТЭК России от 25 декабря 2017 г. № 239)

В значимом объекте не допускаются:

наличие удаленного доступа непосредственно (напрямую) к программным и программно-аппаратным средствам, в том числе СЗИ, для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ

наличие локального бесконтрольного доступа к программным и программно-аппаратным средствам, в том СЗИ, для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ

передача информации, в том числе технологической информации, разработчику (производителю) программных и программно-аппаратных средств, в том числе СЗИ, или иным лицам без контроля со стороны субъекта КИИ

АКТУАЛЬНОСТЬ ДЛЯ ЗАКАЗЧИКА. РАЗВИТИЕ SOC 2.0

Основные решения ИБ

КОМРАД

Визуализация и отчетность

КОМРАД

Управление активами

КОМРАД

Реагирование на инциденты

КОМРАД

Сбор и корреляция событий

Источники событий ИБ

Межсетевое экранирование

РУБИКОН

Антивирусная защита

РУБИКОН

Межсетевое экранирование уровня приложений

Предотвращение утечек информации

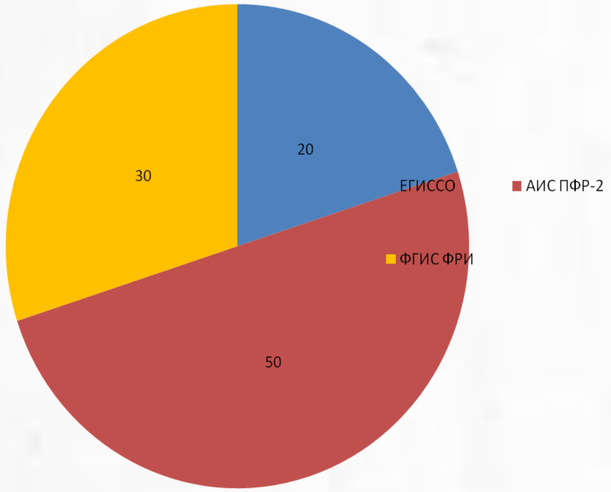
Сканирование сети

Сканер-ВС

ЦЕЛЬ – ОПЕРАТИВНОЕ РЕАГИРОВАНИЕ НА УГРОЗЫ

Количество инцидентов ИБ

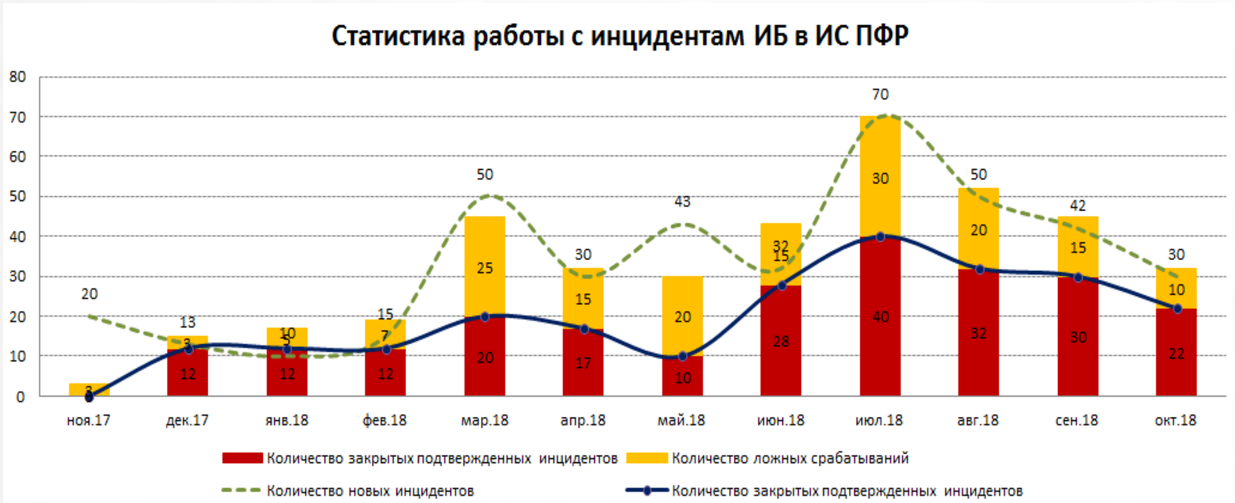
Number of security incidents

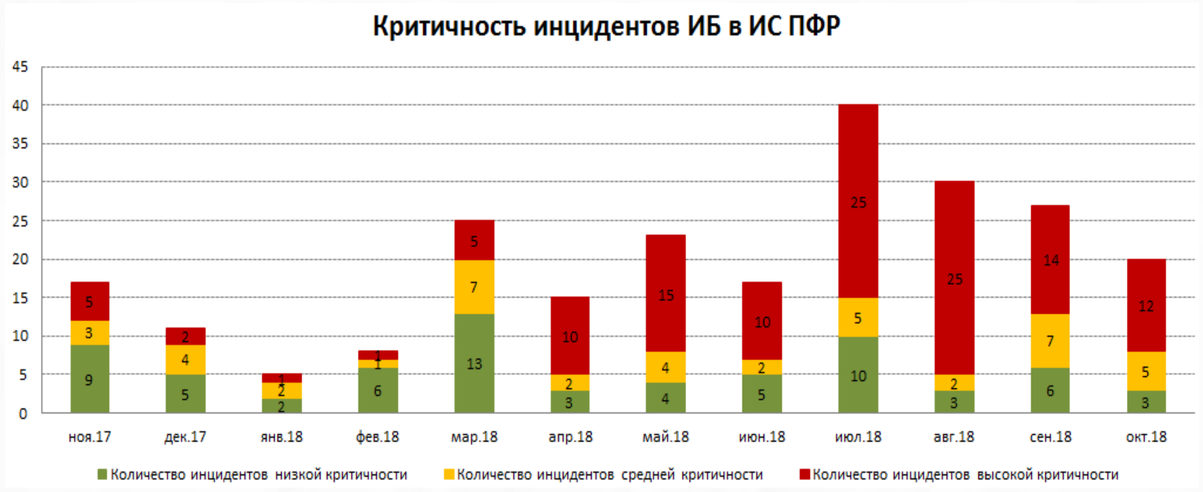


Статистика инцидентов: новые, подтвержденные, закрытые, ложные тревоги

Распределение инцидентов по критичности: высокий, средний, низкий

Распределение инцидентов по типам: подбор паролей, вредоносная активность, несанкционированный доступ и т.п.



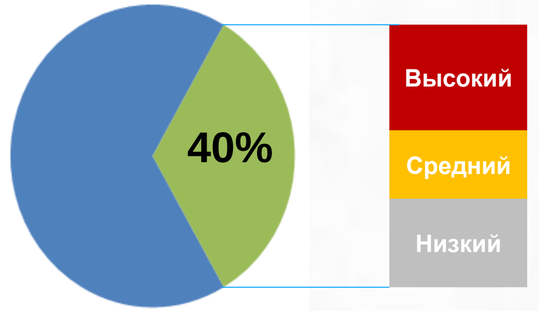


УПРАВЛЕНИЕ ИНЦИДЕНТАМИ БЕЗОПАСНОСТИ

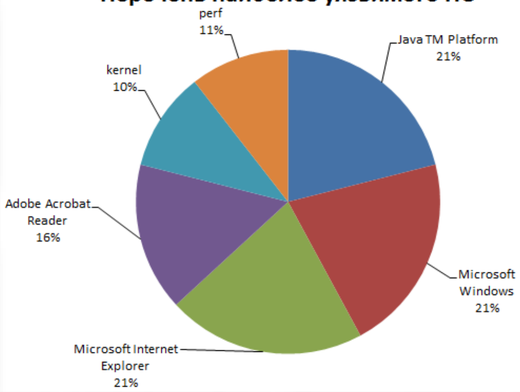
Innopolis University

Инциденты ИБ выявленные/ устраненные	Уязвимости выявленные/ устраненные	Рекомендации по повышению уровня ИБ
Black list	Отсутствие обновлений	Не поддерживаемые ОС
ТОП-10 уязвимых хостов	ТОП-10 критичных уязвимостей	ТОП-10 критичных инцидентов

Количество инцидентов, связанных с низкой осведомленностью в вопросах ИБ

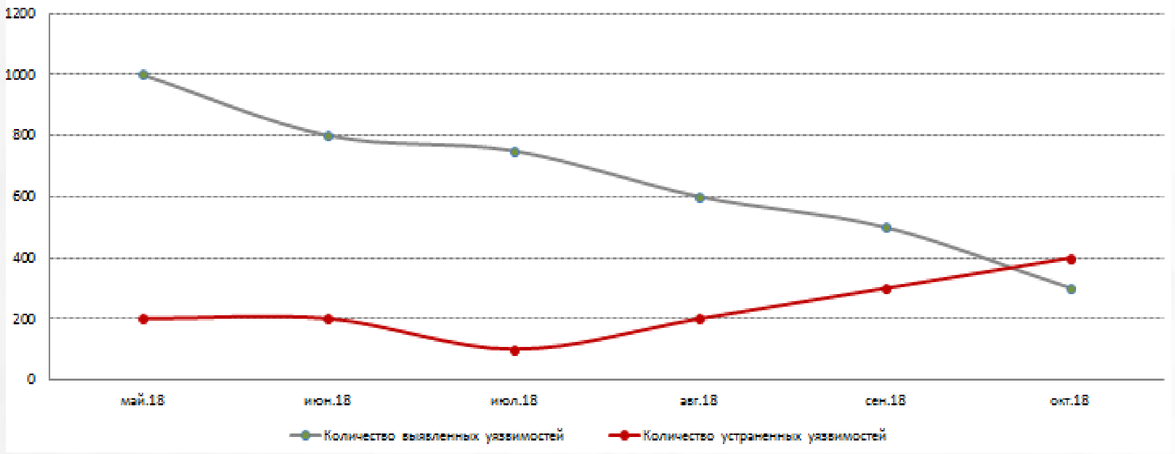


Перечень наиболее уязвимого ПО

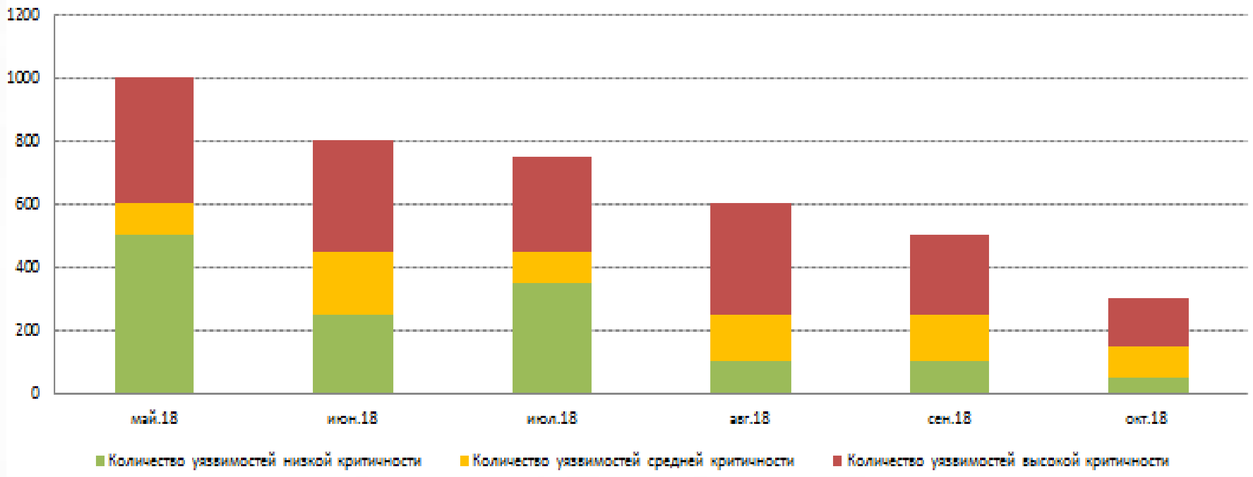


IP	Назначение	Критичность
10.55.0.41	сервер	высокая
10.55.92.12	верт сервер	высокая
10.55.43.24	АРМ	высокая
10.55.3.23	сервер	высокая
10.55.543.34	Сервер	высокая

Управление уязвимостями в ОПФР



Уязвимости в ОПФР



Преимущество решения

Разработанный ПАК принципиально отличается от известных аналогов и систем обнаружения, предупреждения и ликвидаций последствий компьютерных атак (ГосСОПКА) уникальной способностью к самостоятельному ассоциированию и синтезу новых знаний о качественных и количественных характеристик противостояния в киберпространстве Российской Федерации.

Функциональные возможности

Подсистемы ПАК

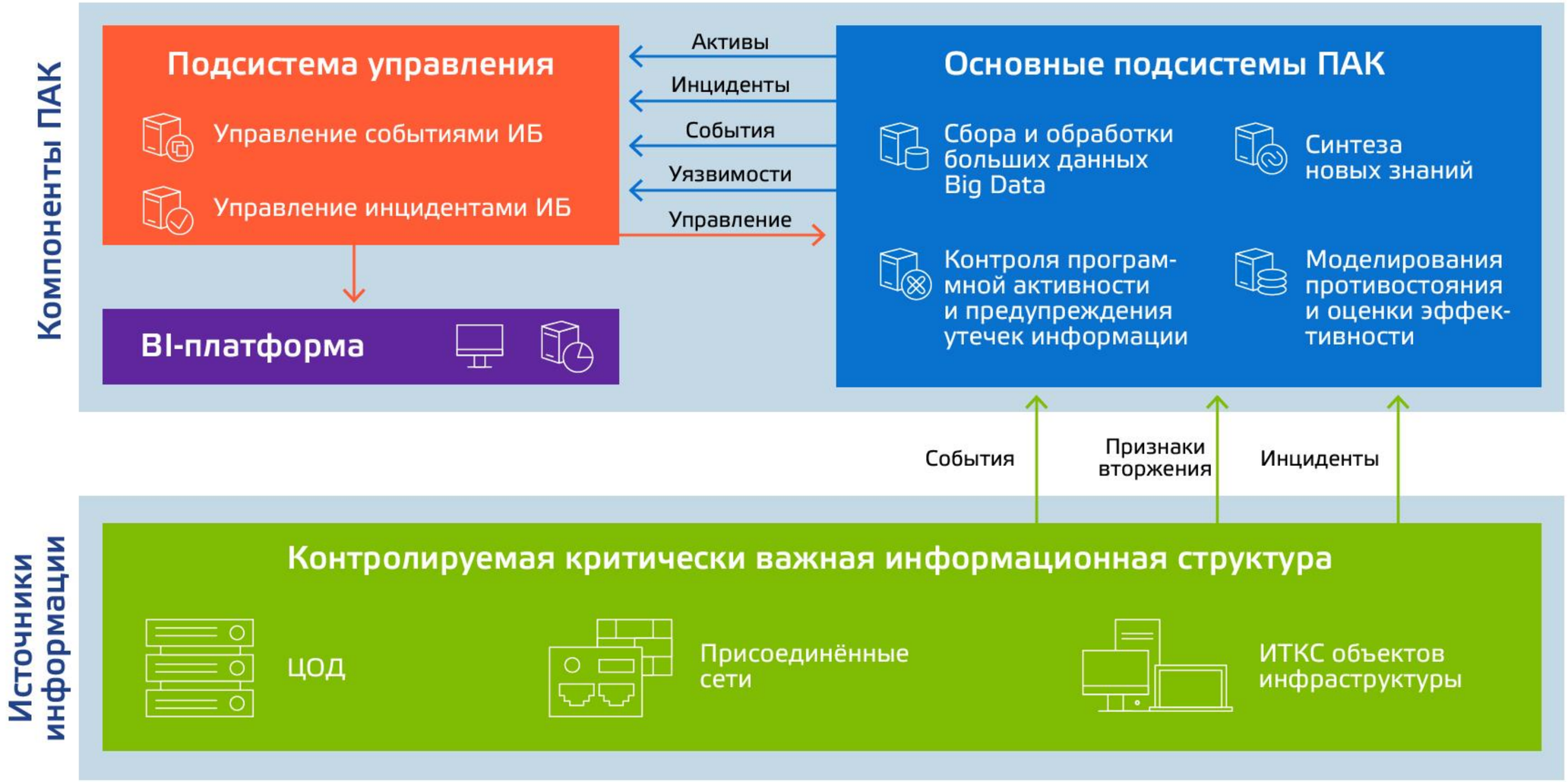
- Единого централизованного мониторинга и управления ИБ
- Межсетевого экранирования и обнаружения вторжений
- Обнаружения аномалий функционирования
- Управления инцидентами ИБ
- Управления событиями ИБ
- Эмуляции критических ресурсов
- Анализа защищенности
- Контроля программной активности
- Статического анализа исходных кодов
- Сбора и обработки больших данных
- Синтеза сценариев предупреждения компьютерного нападения

Назначение

- Управление и мониторинг средств ИБ
- Контроль и фильтрация сетевого трафика
- Обнаружение скрытых угроз в сетевом трафике
- Повышение эффективности обработки инцидентов
- Анализ и корреляция событий ИБ
- Песочница
- Тестирования защищенности информационных систем
- Контроль запуска и выполнения процессов
- Поиск дефектов в исходном коде приложений
- Анализ огромных массивов данных
- Выявление признаков компьютерного нападения

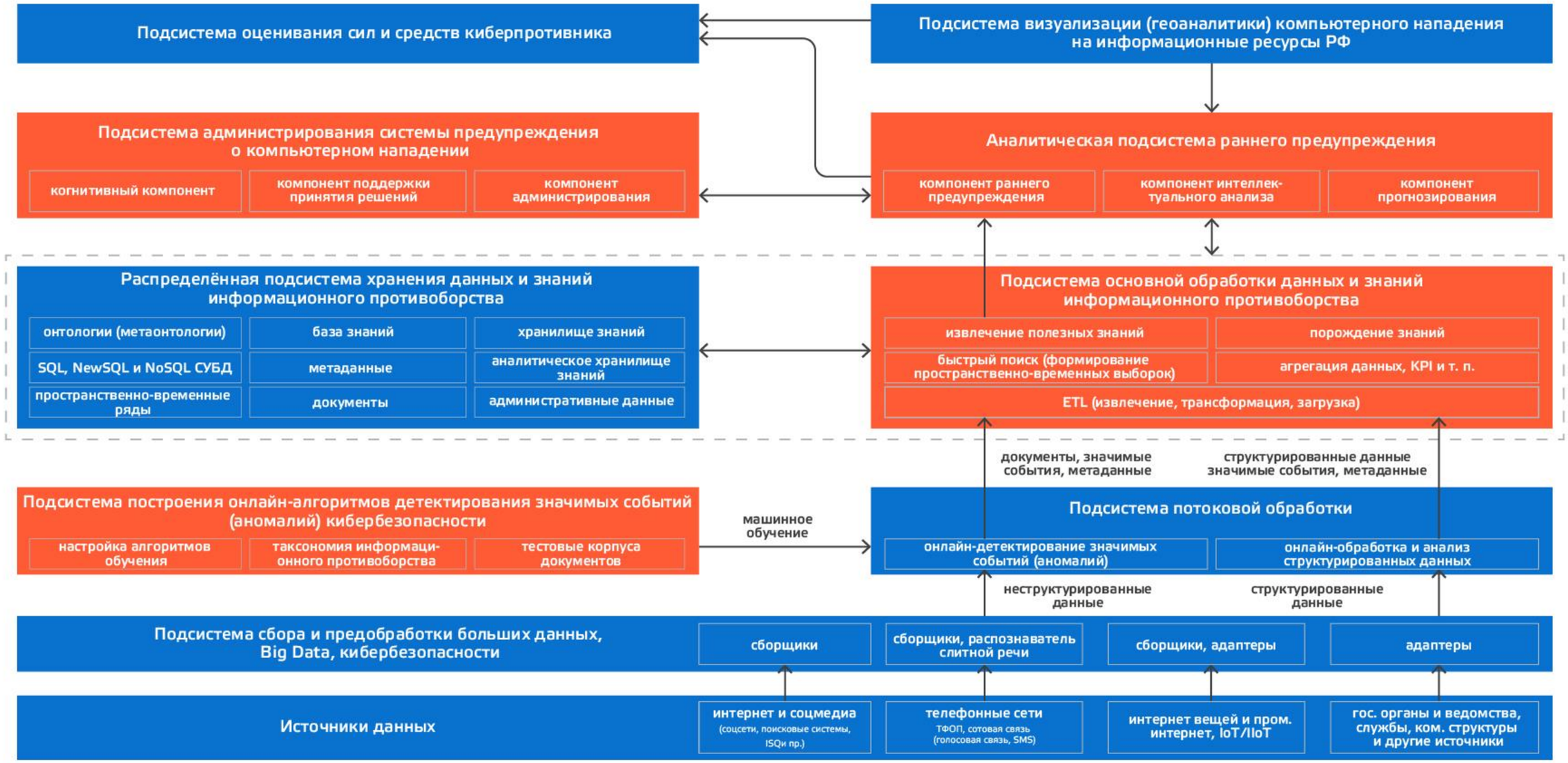
СТРУКТУРНАЯ СХЕМА ПАК

Состав и структура ПАК



ФУНКЦИОНАЛЬНАЯ СХЕМА ПАК

Функциональная схема ПАК



НИОКР ПО СКВОЗНЫМ ТЕХНОЛОГИЯМ КИБЕРБЕЗОПАСНОСТИ

- Разработка новых моделей, методов и средств обеспечения киберустойчивости критической информационной инфраструктуры Российской Федерации, Cyber Resilience ;
- Моделирование обстановки и прогнозирование поведения оппонентов, WarGaming;
- Когнитивные технологии контроля киберпространства и раннего предупреждения компьютерного нападения, iSOPKA;
- Технологии адаптивной архитектуры безопасности, Adaptive Security Architecture;
- Интеллектуальные технологии обеспечения информационной безопасности на основе больших данных и потоковой обработки данных, BigData+ETL;
- Технологии доверенной сетки устройств, Device Mesh и безопасной системной архитектуры, Advanced System Architecture;
- Технологии программно-конфигурируемых сетей, Software Defined Networks (SDN) и виртуализации сетевых функций, Network Functions Virtualization (NFV);
- Технологии криптографических модулей HSM, Hardware Security Module;
- Доверенные «облачные» и виртуальные среды и пр.
- Безопасные мобильные технологии;
- Технологии динамического анализа кода программ;
- Квантовые технологии передачи данных и пр.

НАШИ КНИГИ


River Publishers Series in Security and Digital Forensics
CYBER SECURITY INNOVATION FOR THE DIGITAL ECONOMY
A Case Study of the Russian Federation
Sergei Petrenko
River Publishers


Sergei Petrenko
Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation
Springer


Сергей Петренко, Дмитрий Ступин
Национальная система раннего предупреждения о компьютерном нападении
Сергей Петренко, Дмитрий Ступин
Национальная система раннего предупреждения о компьютерном нападении

Спасибо за внимание!

Петренко Сергей Анатольевич

руководитель Центра ИБ,

Профессор, д.т.н.