INNOPOLIS UNIVERSITY

«Прорывные технологии обеспечения Цифрового суверенитета»

д.т.н., профессор,
руководитель Центра ИБ
Университета Иннополис

Состав Центра ИБ Университета Иннополис

Сергей Анатольевич Петренко

Россия

Конструктор систем безопасности

Доктор технических наук, профессор

❑***Конструктор*** *комплексных систем информационной безопасности критически важных объектов информатизации: трех национальных центров управления, двух доверенных операторов связи MVNO, пяти центров реагирования на инциденты информационной безопасности CERT/CSIRT, более 10 корпоративных и ведомственных сегментов СОПКА и СПОКА.*

❑***Организатор и технический исполнитель*** *более 10 ведомственных и 4 совместных киберучений стран СНГ.*

❑***Эксперт*** *секции по проблемам информационной безопасности научного совета при Совете Безопасности Российской Федерации.*

❑***Научный редактор*** *журнала «Инсайд. Защита информации» (из перечня ВАК РФ). Автор семи монографий и более 250 статей в области информационной безопасности*

❑***Доктор технических наук, профессор***.

❑***Руководитель*** *государственной научной школы «Математическое и программное обеспечение критически важных объектов РФ».*

- **CERT/CSIRT Университета Иннополис**
- **Испытательный полигон для проведения киберучений**
- **Лаборатория практической безопасности IIOT/IoT**
- **Испытательная лаборатория безопасного СПО**
- **Центр подготовки и переподготовки по вопросам информационной безопасности**
- **Лаборатория компьютерной безопасности систем и сетей Internet/Intranet**

INNOPOLIS UNIVERSITY

Основные направления поисковых исследований, R&D Центра ИБ Университета Иннополис

- Разработка экспериментальных полигонов и соответствующего программно-аппаратных комплексов для проведения национальных и международных киберучений;
- Технологии автоматизированного моделирования 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-конфигуриемых 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;
- Безопасные мобильные технологии;
- Технологии динамического анализа кода программ;
- Квантовые технологии передачи данных и пр.

ОТЛИЧИЯ ПРАКТИКИ ЦЕНТРА ИБ УНИВЕРСИТЕТА ИННОПОЛИС ОТ ИЗВЕСТНЫХ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ ШКОЛ

СИНЕРГИЯ НАУКИ И ЛУЧШЕЙ ПРАКТИКИ КИБЕРБЕЗОПАСНОСТИ

- ❑(Академические институты и университеты: ОАО «РТИ», ИСА РАН, ИПУ РАН, ИППИ РАН, СПИИ РАН, Carnegie Mellon University National University of Singapore, Амстердама и пр.)
- ❑Крупные промышленные производители (Yokogawa, Emerson, Siemens, GE, SAP и пр.)
- ❑Отечественные производители средств защиты информации (Лаборатория Касперского, ИнфоТеКС, Позитив, Эшелон и пр.)
- ❑НТИ и Ассоциации IIoT (Сейфнет, Нейронет, Аэронет, Консорциум IIoT, Ассоциация IIoT и пр.)

Стадия	Основные этапы
Ранняя: **И**ниициация задач практической безопасности	-Привлечение ведущих ученых, отдельных исследовательских групп -Привлечение к проблеме внимания отдельных исследователей -Организация семинаров, конференций и круглых столов по проблемам безопасности
Поздняя: Выполнение поисковых исследований в области безопасности	- Научно-технический консалтинг - Выполнение наукоемких проектов безопасности - Научно-техническое сопровождение - Подготовка и переподготовка Заказчика

Подбор квалифицированных исполнителей НИОКР

Подбор руководителей проектов

Выполнение и научно-техническое сопровождение комплексных решений безопасности

Проведение углубленной экспертизы и консультаций

Киберзащита выделенного объекта информатизации

Решение задачи защиты выделенного объекта информатизации от угроз информационной безопасности.

Традиционный подход обеспечения ИБ

- Развертывание межсетевых экранов;
- Использование систем антивирусной защиты;
- Оснащение модулями доверенной загрузки;
- Внедрение система разграничения доступа.

Назначение решения

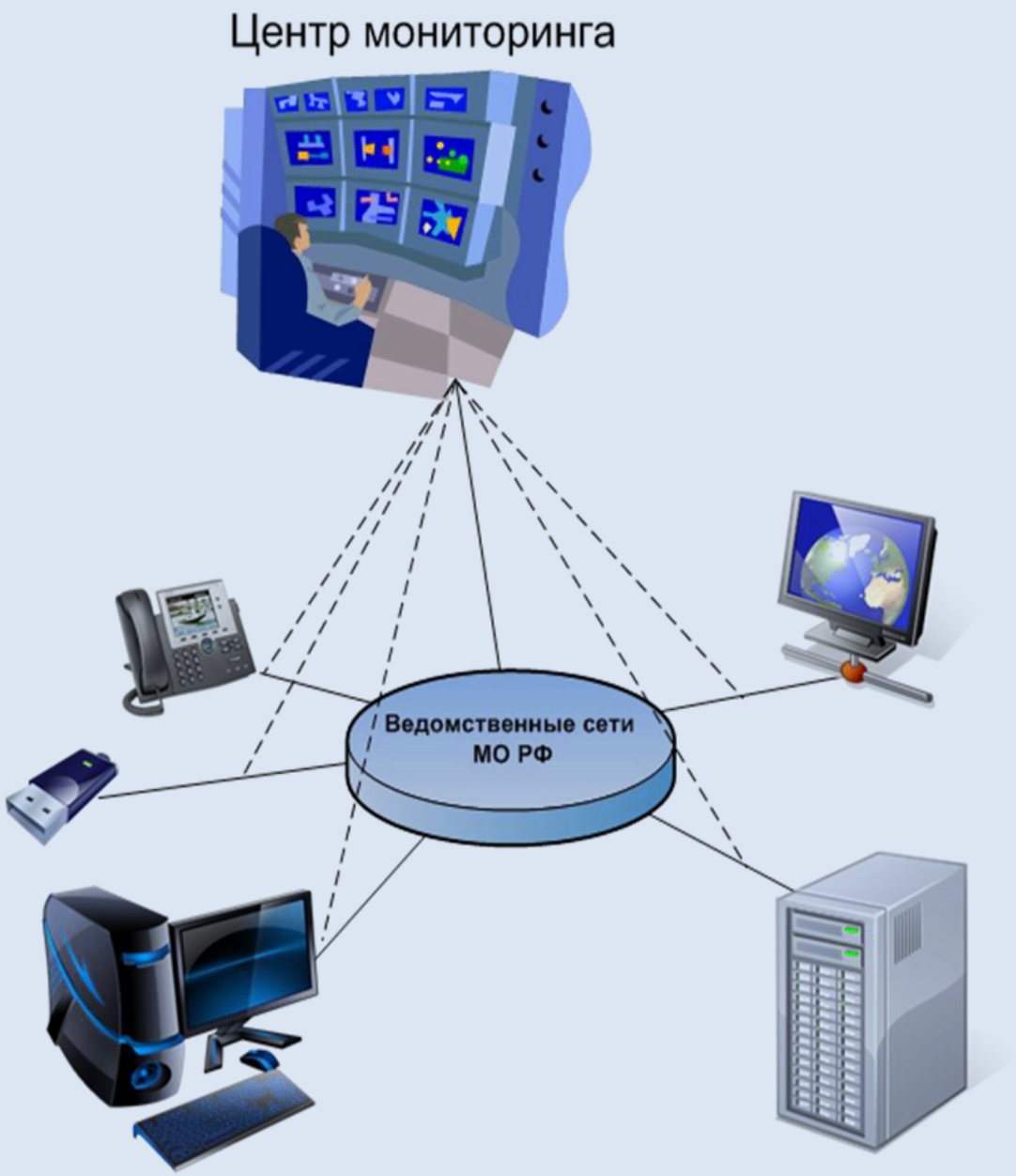
- Обеспечение информационной безопасности выделенного объекта;
- Решение вопросов разбора инцидентов и аудита информационной безопасности;
- Обеспечение разграничений доступа к внутренним информационным ресурсам.

Предложения

- Создание систем кибербезопасности, основанных на современных информационно-телекоммуникационных технологиях;
- Разработка предложений по киберзащите критически важных объектов и информационных ресурсов;
- Создание локальных центров мониторинга событий информационной безопасности;
- Внедрение систем защиты от утечек информации;
- Развертывание систем анализа уязвимостей;
- Разработка система контроля пользователей и аномального поведения.

Киберзащита сетевой инфраструктуры

Решение задачи защиты ведомственного или корпоративного сегмента сетевой инфраструктуры



Назначение решения

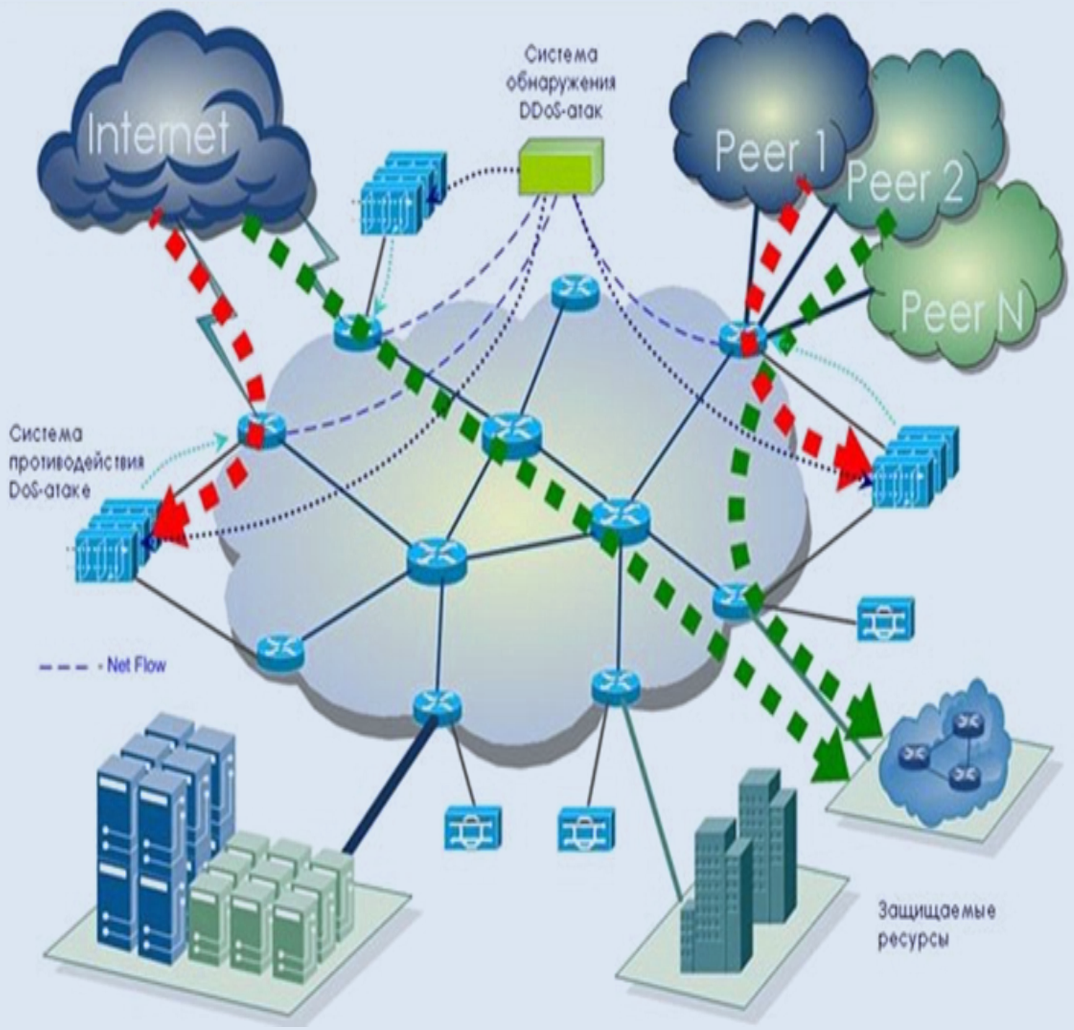
- Разработка системы защиты от актуальных кибератак и внутренних угроз сетевой инфраструктуры;
- Решение вопросов интеграции различных систем безопасности в единый центр мониторинга;
- Обеспечение единой системы управления политиками безопасности в рамках закрытого и открытого сегментов сети.

Предложения

- Создание инфраструктуры центра управления в составе ситуационного центра
- Информационное сопряжение сил войск информационных операций с системами кибербезопасности других силовых структур, обеспечивающих безопасность РФ;
- Разработка защиты систем документооборота (СЭД) и других ключевых информационных ресурсов.

Мониторинг киберпространства РФ

Мониторинг за глобальными информационными сетями с целью обеспечения безопасности критически важных объектов информатизации РФ.



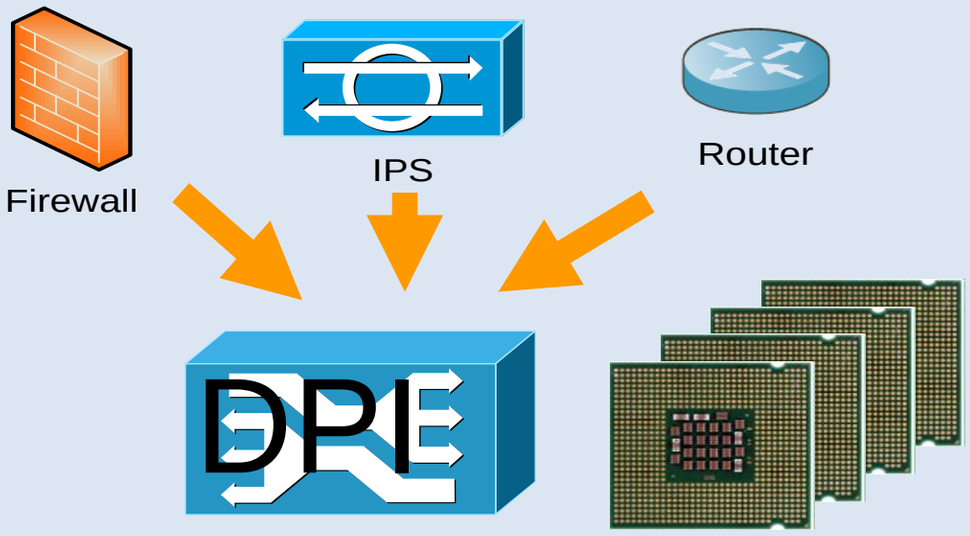
Назначение решения

- Мониторинг и своевременное реагирование на уровень угроз кибербезопасности в сети Интернет;
- Обеспечение возможности контроля и мониторинга киберпространства;
- Создание единого центра мониторинга киберпространства.

Предложения

- Развертывание элементов контроля за узлами глобальной информационных систем;
- Внедрение доверенного оборудования на узлах международного присутствия;
- Создание единой системы мониторинга за ключевыми узлами Интернет;
- Обеспечение работы систем защиты от глобальных вирусных угроз и кибератак;
- Разработка системы аномального поведения на глобальных сетях передачи данных.

«Глубокий» анализ трафика (DPI – Deep Packet Inspection)



Назначение решения

Deep Packet Inspection - технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому.
DPI является ключевой частью систем защиты от киберугроз, систем предотвращения утечек информации, систем защиты от DDoS и др.

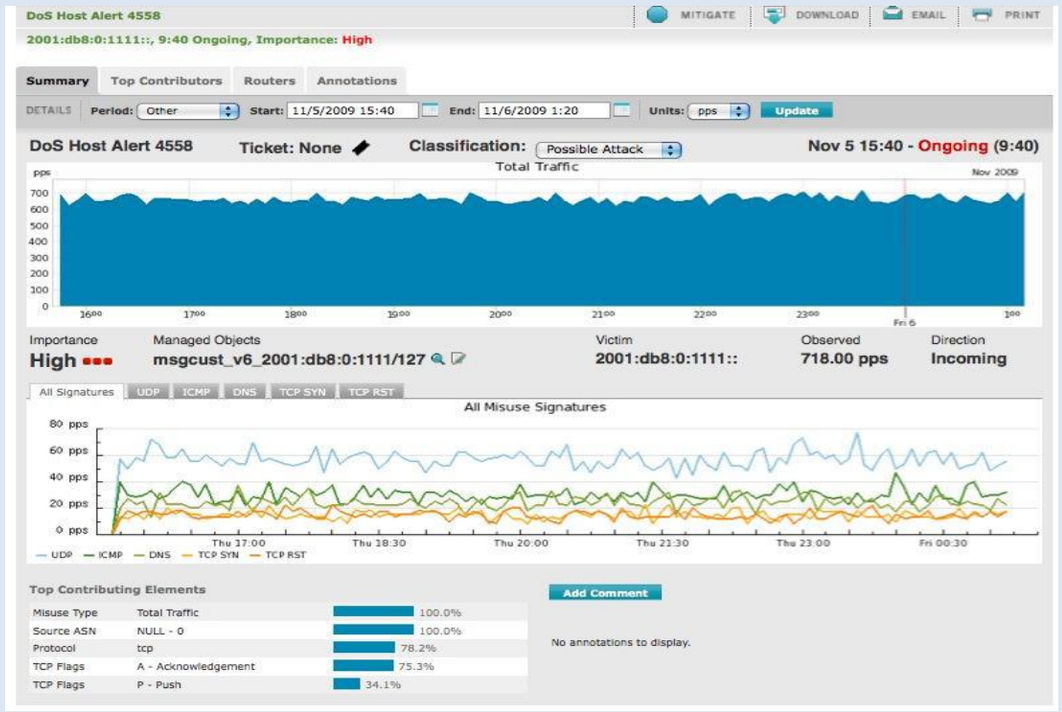
Функционал и параметры DPI

- Анализ протоколов на уровне L2-L7;
- Поддержка большинства сетевых протоколов;
- Возможность задания фильтров шаблонов для анализа;
- Варианты включения в сеть в качестве “зеркала”, “блокировки” и “в разрыв”;
- Линейка решений с интерфейсами 10Gb, 40Gb, 100Gb; Возможность блокировки нежелательных Интернет-ресурсов из «черных списков»;
- Защита пользователей оператора связи от распределенных атак (DDoS-атак)..

Преимущества решения

Разработка отечественной платформы DPI позволит избежать внедрение программных закладок и недокументированных возможностей в ключевом элементе кибербезопасности. Кроме того, наличие собственной платформы DPI позволит оперативно вносить изменения в программную часть и создавать собственные, более точные, правила работы.

Зашита от групповых и массовых кибератак, DDoS, APT и пр.



Назначение решения

Предлагается:

- Организовать работу по координации деятельности операторов связи и специализированных организаций по выявлению и пресечению DDoS-атак;
- Выявить перечень ресурсов, подлежащих обязательной защите;
- Разработать или выбрать и сертифицировать из имеющихся на рынке отечественных решений по защите от DDoS-атак;
- Создать комплексную государственную систему защиты от DDoS-атак.

Традиционный подход

- Обнаружение и отчеты по статистическим аномалиям;
- Аномалии обнаруживаются, классифицируются и отслеживаются в реальном времени;
- Подавление при необходимости:
  - ACL, BlackHole, FlowSpec;
  - Интеллектуальные системы.

Преимущества решения

- Модель очистки «по запросу»;
- Противодействие нескольким атакам одновременно; Защита от уровня протокола до уровня сервиса;
- Контроль и управление противодействием в реальном времени;
- Единая графическая консоль для обнаружения и противодействия;
- Скорости от 10 до 400 Гбит/с на устройство.

Реагирование на инциденты компьютерной безопасности

Централизованная информационная система для обработки инцидентов безопасности на организационном и техническом уровнях.

Задачи системы управления событиями ИБ

- Консолидация и хранение журналов событий различных источников;
- Предоставление инструментов для анализа событий и разбора инцидентов;
- Корреляция и обработка событий по заданным правилам;
- Автоматическое оповещение персонала об инцидентах безопасности.

Назначение решения

- Обнаружение инцидентов безопасности;
- Уменьшение последствий инцидента безопасности;
- Увеличение эффективности системы безопасности;
- Учет деятельности персонала и процессов;
- Отработка инцидентов безопасности (тренинги).

Преимущества решения

- Доверенное программное обеспечение;
- Современный математический аппарат;
- Полноценная поддержка любого оборудования;
- Удобный пользовательский интерфейс;
- Гибкий механизм построения отчетов;
- Производительность высоконагруженных систем.

Создание баз угроз безопасности и уязвимостей критической инфраструктуры

Централизованная система мониторинга ведомственных, операторских и промышленных систем управления событиями безопасности для раннего обнаружения кибератак федерального масштаба.

Назначение решения

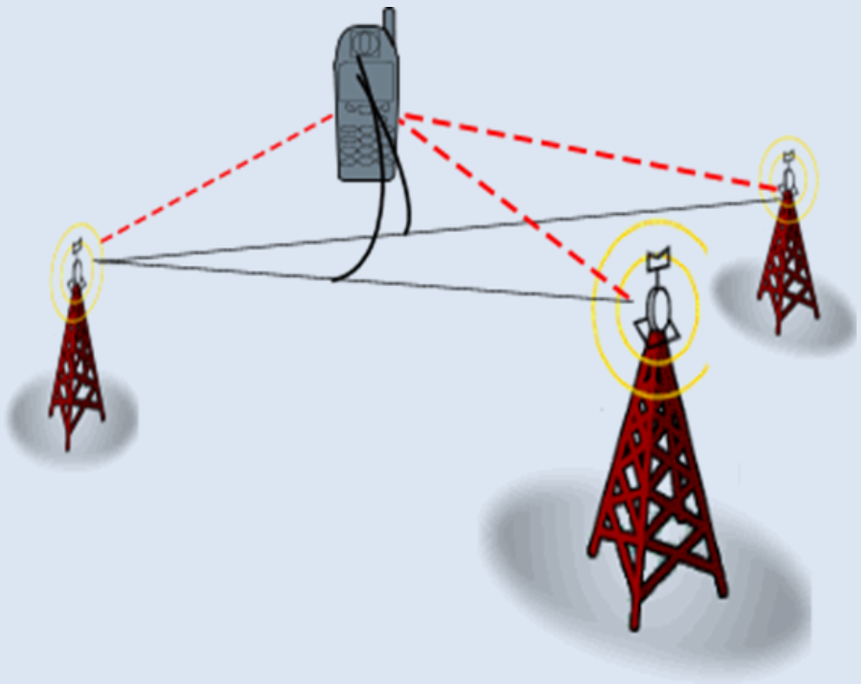
- Организация единой базы инцидентов безопасности;
- Мониторинг и своевременное обнаружение атак на важные объекты;
- Обеспечение возможности предотвращения последующих атак.

Предложения

- Создание защищенного ЦОД;
- Разработка доверенного программного обеспечения для сбора информации об инцидентах безопасности;
- Разработка модулей совместимости с действующими системами управления событиями безопасности;
- Создание средств анализа текущих инцидентов безопасности.

Гео-позиционирование абонентов

Создание платформы гео-позиционирования мобильных абонентов в сотовых сетях связи



Назначение решения

- Определение географических координат абонентов;
- Оценка местоположения абонентской базы в целом;
- Исследование регулярных перемещений абонентской базы;
- Отслеживание местоположения абонентов за определенный промежуток времени;
- Оповещение абонентов с помощью SMS по территориальному признаку;

Постановка задачи

Мобильные устройства широко распространены и обладают значительной мощностью, что делает их привлекательным объектом и/или ресурсом для проведения кибератак.

Преимущества решения

- Охват всей территории покрытия и всех абонентов сети;
- Возможность работы с абонентами в роуминге по общеканальной сигнализации сотовой связи;
- Система аналитических сервисов для решения специальных задач.

«Глубокое» профилирование субъектов и объектов наблюдения

Назначение решения

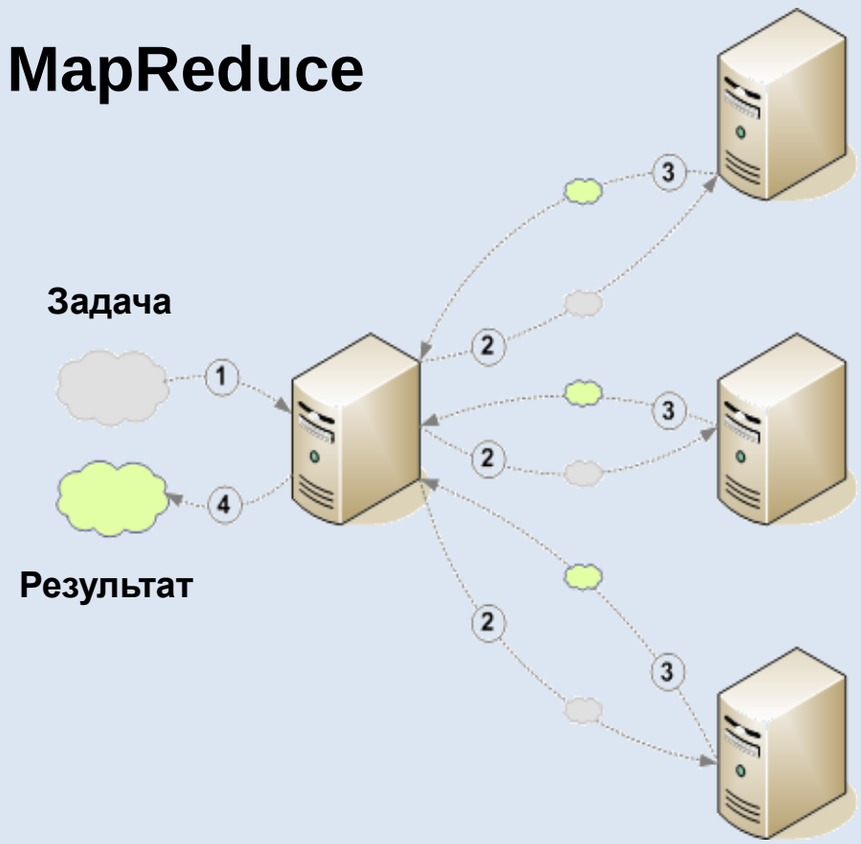
- Построение профиля пользователя, сбор всей имеющейся о нём информации с целью получения электронного досье;
- Анализ отклонений в поведении групп пользователей и выявление вызвавших это причин с целью получения информации о планируемых и произошедших событиях;
- Контроль за поведением групп, специализирующихся на определённой тематике и анализ публикуемой в них информации с целью получения фото, видео материалов и печатных документов.

Предложения

- Создание сервиса мониторинга открытых и частных источников информации на предмет появления интересующих данных;
- Контроль за тенденциями и построение прогнозов развития событий;
- Обеспечение оперативного получение структурированной информации по заданным запросам.

Обработка больших данных (BigData)

Для хранения и обработки больших объемов информации (петабайты), полученных из **социальных сетей,** систем **DPI** и других систем мониторинга **требуются** специальные вычислительные комплексы – кластеры, а также специализированное программное обеспечение – базы данных типа NoSQL и эффективные алгоритмы параллельных вычислений MapReduce.



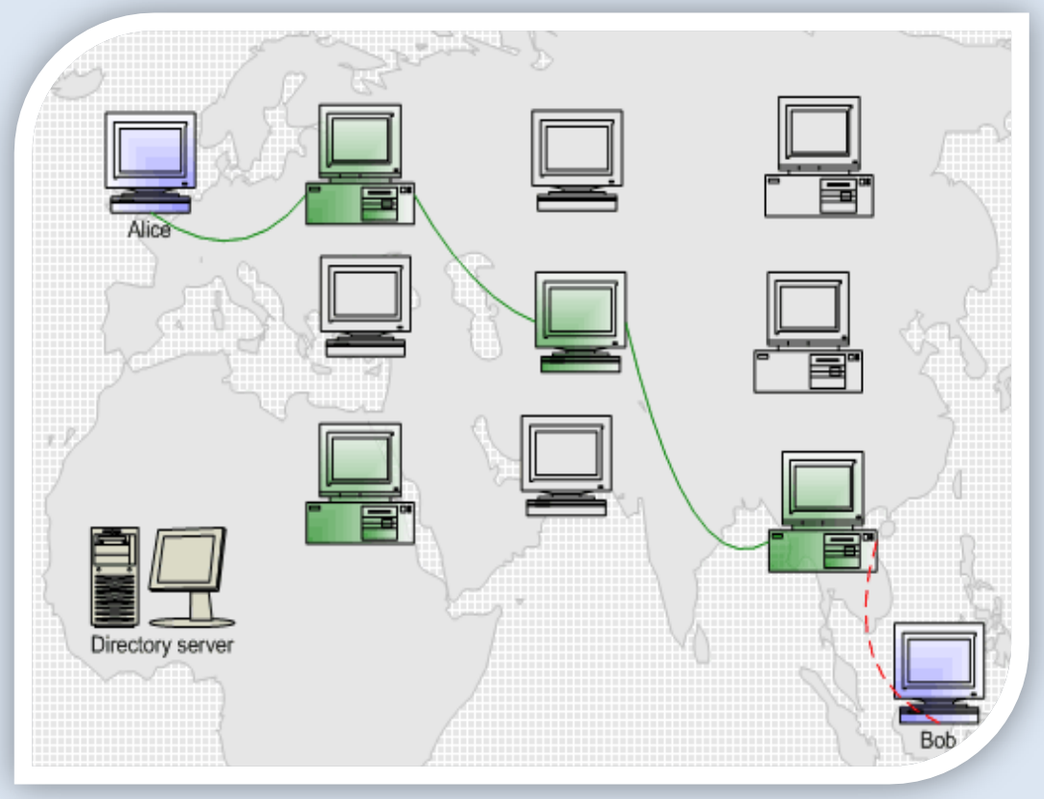
Базы данных типа NoSQL

- Большой объем данных;
- Высокая скорость обработки данных;
- Многообразие одновременно обрабатываемой информации;
- Хорошая горизонтальная масштабируемость.

Предложения

- Развертывание элементов контроля за узлами глобальной информационных систем;
- Внедрение доверенного оборудования на узлах международного присутствия;
- Создание единой системы мониторинга за ключевыми узлами Интернет;
- Обеспечение работы систем защиты от глобальных вирусных угроз и кибератак;

Исследование TOR-сетей и определение источников кибератак



Назначение решения

- Определение источников кибератак;
- Определение и анализ анонимайзеров;
- Разработка методов выявления источников киберугроз;
- Разработка методов проведения расследования инцидентов
- Подготовки инструментария проведения ответных или превентивных контрмер.

Постановка задачи

TOR - сеть это одна из самых известных сетей анонимного доступа, работающая по протоколу SOCKS. Данная сеть служит для сокрытия факта связи клиента и сервера и использует в своей работе криптографические методы, основанные на инфраструктуре открытых ключей.

Предложения

- Контроль за трафикам в узлах tor-сетей;
- Определение корреляции анонимного и не анонимного трафика;
- Проведение исследования времен задержки (timing attack);
- Применение статистических методов анализа;
- Использование уязвимостей в ПО TOR-клиентов и прокси-серверов.

Создание банка данных по актуальным киберугрозам и уязвимостям

Назначение решения

Система агрегации предназначена для сбора, накопления и обработки актуальной информации об уязвимостях, вирусных атаках, бот сетях, зараженных публичных ресурсах, хакерских командах и их акциях. Информация в данную систему поступает из открытых источников, разработчиков антивирусного ПО и средств информационной защиты, исследовательских центров.

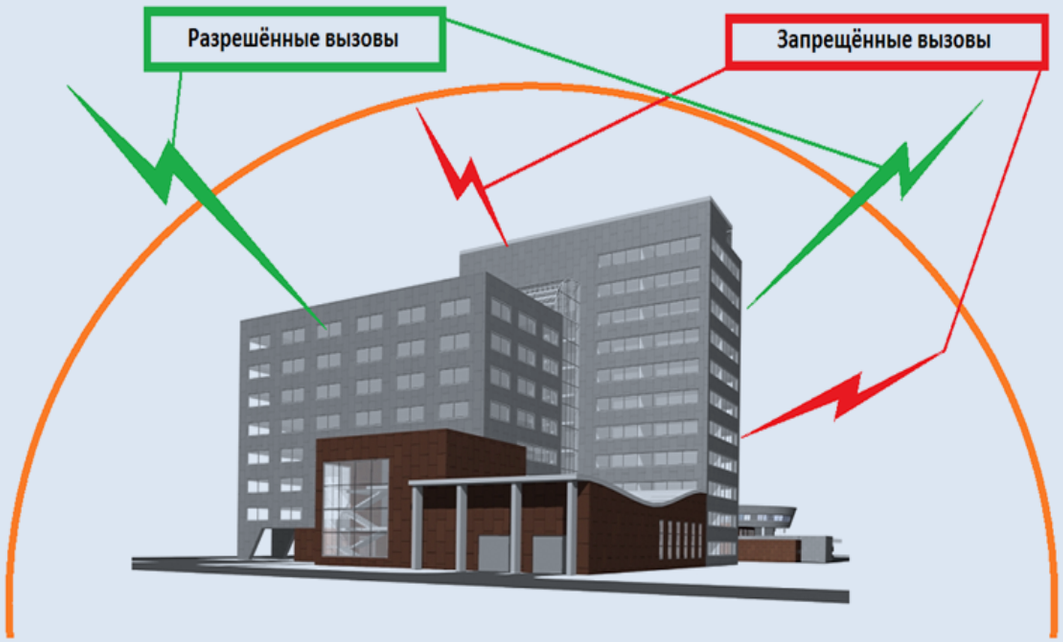
Постановка задачи

Наличие уязвимостей и недокументированных возможностей в ПО, в аппаратных модулях, в средствах защиты являются основным источником киберугроз и средством распространения вредоностного и шпионского ПО.

Предложения

- Создание базы данных актуальных уязвимостей;
- Использование данных открытых источников;
- Использование Испытательной лаборатории для пополнения данных об уязвимостях;
- Подготовка базиса для проведения специальных операций;
- Интеграция с существующими российскими центрами мониторинга и ведущими антивирусными лабораториями.

Создание доверенного цифрового периметра



Назначение решения

- Построения участков доверенной сети конфиденциальной мобильной связи на объектах особой ответственности, зонах чрезвычайных ситуаций и других специальных объектах;
- Полный контроль за обменом информации между сетью общего пользования и защищаемой подсетью;
- Экстренное оповещение мобильных абонентов операторов связи.
- Определение координат абонента с точностью до помещения.

Постановка задачи

- Широкое распространение мобильных телефонов и других беспроводных устройств;
- Недоверенное программное и аппаратное обеспечение мобильных платформ;
- Уязвимости в ПО;
- Недостаточность административных мер;
- Наличие камер и других средств съема информации.

Преимущества решения

- Все компоненты комплекса полностью отечественного производства;
- Позволяет разрешать/запрещать переговоры определенным абонентам и организовывать приоритезацию абонентов;
- Интеграция с сетью провайдера связи;
- Различные варианты исполнения от мобильного до стационарного.

Внедрение доверенной беспроводной сети передачи данных

Назначение решения

Беспроводная сеть связи позволяет осуществлять передачу:

- IP-телефонии;
- Видео-сигнала, видеоконференции;
- Электронная почта, календарь, планировщик;
- Документооборот;
- Специализированное сетевого программного обеспечение.

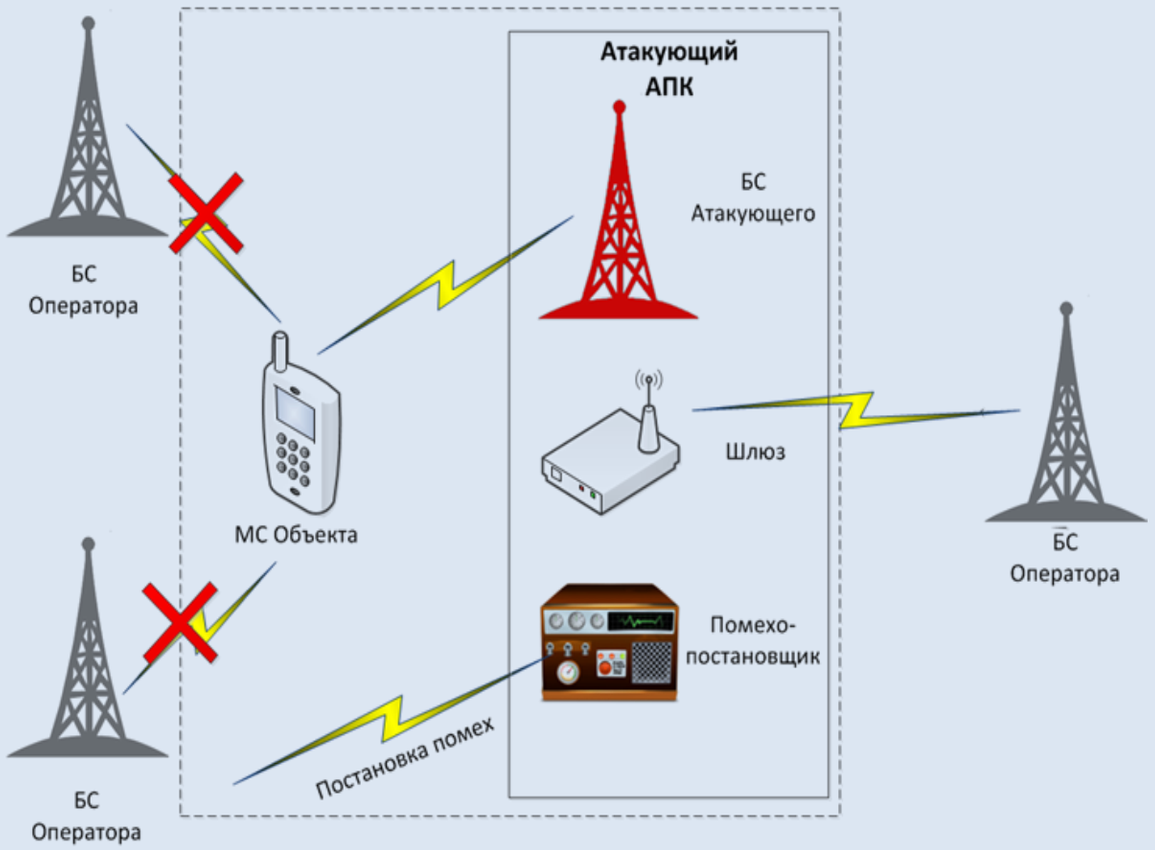
Постановка задачи

- Необходимость в доверенном широком канале связи;
- Переход на системы электронного документа оборота и мобильные рабочие места;
- Необходимость передачи видео, аудио контента и других данных большого объема.

Преимущества решения

- Высокоскоростная широкополосная беспроводная сеть связи Wi-Fi;
- Проверенное, сертифицированное оборудование:
  - сетевые роутеры,
  - USB-адаптеры,
  - смартфоны и т.п.
- Российские криптографические алгоритмы.

Разработка перспективных методов мониторинга сетей беспроводной связи



Назначение решения

Разработка перспективных методов мониторинга позволит выполнять ряд задач по перехвату, дешифрованию и анализу данных, передаваемых в беспроводных высокоскоростных широкополосных сетях передачи данных за время близкое к реальному.

Разрабатываемые сети связи

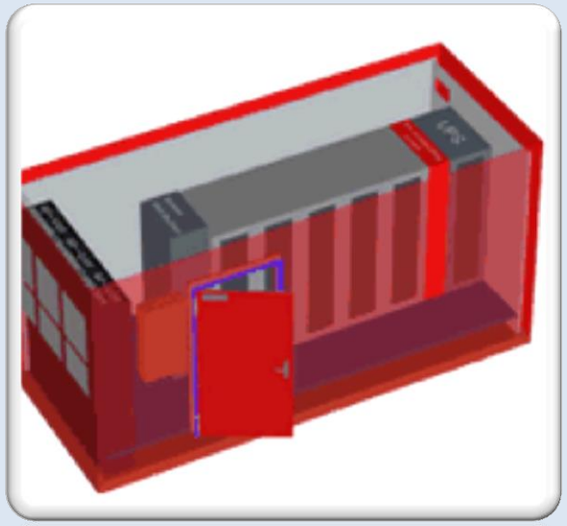
- Сотовые сети стандарта GSM 2G;
- Сотовые сети стандарта GSM 3G;
- Сотовые сети стандарта 4G (LTE) и 5G;
- Беспроводные сети Wi-Fi.

Преимущества решения

- Анализ публичных, частных и корпоративных сетей Wi-Fi с целью сбора данных;
- Перехват, подмена и навязывания сообщений;
- Контроль голосового трафика и трафика данных;
- Определение и сокрытие местоположения абонентов.

Повышение мобильности и оперативности командных центров

Разработка возимых узлов (ВУ) различного назначения на базе единой платформы для перевозки авиа, морским, жд и авто-транспортом для лиц принимающих решения в полевых условиях



Назначение решения

Разработка на базе единой платформы:

- Возимого узла мониторинга угроз ИБ;
- Возимого узла предупреждения кибератак;
- Возимого ситуационного центра реагирования на инциденты компьютерной безопасности.

Возимые узлы обеспечат быструю транспортировку и развертывание упомянутых центров в полевых условиях (киберучения, обеспечение деятельности и пр.).

Предложения

Возимый узел предоставляет:

- От 6 до 30 (в зависимости от оснащённости и назначения) рабочих мест операторов;
- Доступ к открытой и\или закрытой телефонной связи;
- Доступ к открытой и\или закрытой электронной почты, СЭД и интернет;
- Доступ к открытой и\или закрытой видеоконференцсвязи.

Создание специальных тренажеров и полигонов

Новейшие программно-аппаратные комплексы, центры обработки данных, центры мониторинга и прочие объекты инфраструктуры киберзащиты требуют хорошо обученный персонал. Для подготовки кадрового состава необходимо создание специального центра подготовки.

Назначение решения

- Обучение персонала объектов использованию новых программно-аппаратных комплексов;
- Проведение групповых тренировок и учений;
- Аттестация персонала;
- Организация учений.

Предложения

- Создание Учебного центра;
- Собственная Испытательная лаборатория;
- Разработка программ обучения персонала;
- Сотрудничество с ведущими ВУЗами страны;
- Исследование новейших и перспективных образцов техники и средств связи;
- Поиск и проверка уязвимостей в ПО, средств проникновения, вирусов.

Дополнительные источники информации

INNOPOLIS UNIVERSITY

Руководитель Центра ИБ,

Конструктор систем кибербезопасности,

д.т.н., профессор

Сергей Петренко

s.petrenko@innopolis.ru