Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

ИНФОКОММУНИКАЦИИ

**56-я научная конференция
аспирантов, магистрантов и студентов**

Сборник тезисов докладов

18–20 мая 2020 года
Минск, БГУИР

УДК 621.391

56-я юбилейная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 18-20 мая 2020 г., БГУИР, Минск, Беларусь: тезисы докладов. – Мн. – 2020. – 173 с.; ил.

В сборнике опубликованы тезисы докладов, представленных на 56-й научной конференции аспирантов, магистрантов и студентов БГУИР. Материалы одобрены оргкомитетом и публикуются в авторской редакции.

Для научных и инженерно-технических работников, преподавателей, аспирантов, магистрантов и студентов вузов.

СОДЕРЖАНИЕ

УЯЗВИМОСТИ ARP И DNS В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Аблецов А.М

Белоусова Е.С – к.т.н., доцент

В работе рассматриваются уязвимости протоколов ARP и DNS в локальных вычислительных сетях. Для практической реализации атак использовалась утилита Ettercap. Также представлены рекомендации для исключения выявленных уязвимостей в локальных вычислительных сетях.

Локальная вычислительная сеть (англ. Local Area Network, LAN) – сеть, соединяющая оконечные устройства, расположенные на относительно небольшом расстоянии друг от друга (дом, офис, административное здание), с целью повышение эффективности работы оконечных устройств за счет совместного использования ресурсов, а также для доступа в глобальную вычислительную сеть (англ. Wide Area Network, WAN).

Сетевые протоколы, используемые для связи устройств в LAN и WAN были разработаны в конце XX, так например протокол ARP был внедрен в 1982 г., DNS – в 1983 г., DHCP – в 1990 г. Основными требованиями для данных протоколов были производительность и эффективность. Вопросам защиты информации уделялось незначительное внимание. Из этого следует, что сетевые протоколы обладают рядом уязвимостей.

Для демонстрации уязвимостей была использована схема, представленная на рисунке 1, которая реализует атаку «Человек по середине» (англ. Man In The Middle, MITM).

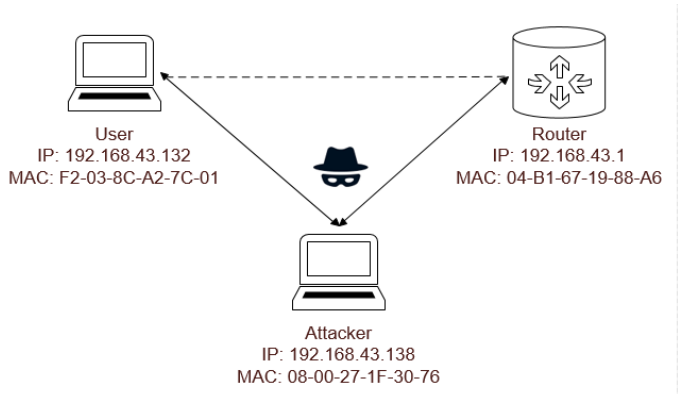


Рисунок 1 – Схема построения сети для демонстрации атаки MITM

Одним из основных протоколов LAN является ARP, предназначенный для сопоставления IP-адресам MAC-адресов. Информация об этих сопоставлениях хранится в оперативной памяти оконечных устройств (ARP-кэш). Протокол не предполагает какой-либо аутентификации. Следовательно, злоумышленник, инициализируя заведомо ложные ARP фреймы, способен изменить ARP-кэш устройств, находящихся с ним в пределах одной LAN, что используется для перенаправления трафика и реализации атаки MITM.

Для использования данной уязвимости злоумышленник (Attacker) с помощью утилиты Ettercap [1] изменил ARP-кэш на устройстве пользователя (User). На рисунке 2 представлен ARP-кэш до и после проведения атаки на устройстве User. Теперь весь трафик, направляемый в WAN от устройства User, проходит через устройство Attacker

```
C:\Users\admin>arp -a

Interface: 192.168.43.132 --- 0x2
  Internet Address      Physical Address      Type
  192.168.43.1          04-b1-67-19-88-a6     dynamic
  192.168.43.138        08-00-27-1f-30-76     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
```

```
C:\Users\admin>arp -a

Interface: 192.168.43.132 --- 0x2
  Internet Address      Physical Address      Type
  192.168.43.1          08-00-27-1f-30-76     dynamic
  192.168.43.138        08-00-27-1f-30-76     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
```

Рисунок 2 – ARP кэш на устройстве User до и во время проведения атаки соответственно

На рисунке 3 представлен процесс формирование устройством Attacker ложных ARP фреймов, который может быть отслежен с помощью сетевого анализатора Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
35	1.850110014	PcsCompu_1f:30:76	f2:03:27:a2:08:3e	ARP	42	192.168.43.1 is at 08:00:27:1f:30:76
36	1.850184590	PcsCompu_1f:30:76	XiaomiCo_19:88:a6	ARP	42	192.168.43.132 is at 08:00:27:1f:30:76 (duplicate use…
37	1.860383541	PcsCompu_1f:30:76	XiaomiCo_19:88:a6	ARP	42	192.168.43.132 is at 08:00:27:1f:30:76 (duplicate use…
38	1.860434579	PcsCompu_1f:30:76	f2:03:27:a2:08:3e	ARP	42	192.168.43.1 is at 08:00:27:1f:30:76
39	11.870838430	PcsCompu_1f:30:76	f2:03:27:a2:08:3e	ARP	42	192.168.43.1 is at 08:00:27:1f:30:76
40	11.870892220	PcsCompu_1f:30:76	XiaomiCo_19:88:a6	ARP	42	192.168.43.132 is at 08:00:27:1f:30:76 (duplicate use…
41	11.881087308	PcsCompu_1f:30:76	XiaomiCo_19:88:a6	ARP	42	192.168.43.132 is at 08:00:27:1f:30:76 (duplicate use…
42	11.881126702	PcsCompu_1f:30:76	f2:03:27:a2:08:3e	ARP	42	192.168.43.1 is at 08:00:27:1f:30:76

Рисунок 3 – Формирование ложных ARP фреймов злоумышленником

В качестве примера было организовано HTTP соединение устройства User с интернет ресурсом, а также аутентификация пользователя. С помощью сетевого анализатора Wireshark, устройство Attacker просматривает содержимое перенаправленного трафика. Результат перехвата логина и пароля пользователя представлены на рисунке 4.

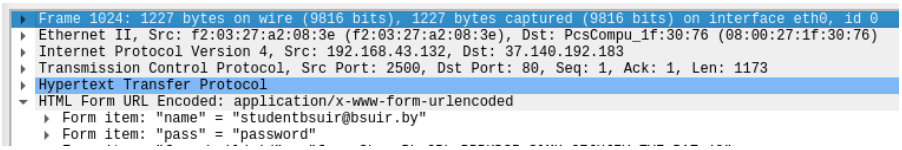


Рисунок 4. Результат перехвата пароля пользователя

Также с помощью уязвимости протокола ARP злоумышленник имеет возможность провести DNS-атаку. Протокол DNS предназначен для сопоставления IP-адресам доменных имен. Информация об этих сопоставлениях хранится в виде DNS-кэша на оконечных устройствах. Изменяя DNS-кэш, злоумышленник может перенаправить запрос пользователя на заведомо ложный IP-адрес.

Для проведения данной атаки устройство Attacker, с помощью утилиты Ettercap изменяет ARP-кэш на устройстве User. Затем, выступая в роли DNS-сервера, сопоставляет свой IP-адрес доменному имени, введенному на устройстве User. Таким образом, DNS-атака может применятся с целью вымогания денег, а также в качестве атаки «Отказ в обслуживании». На рисунке 5 представлены неудачные попытки устройства User получить доступ к интернет ресурсам.

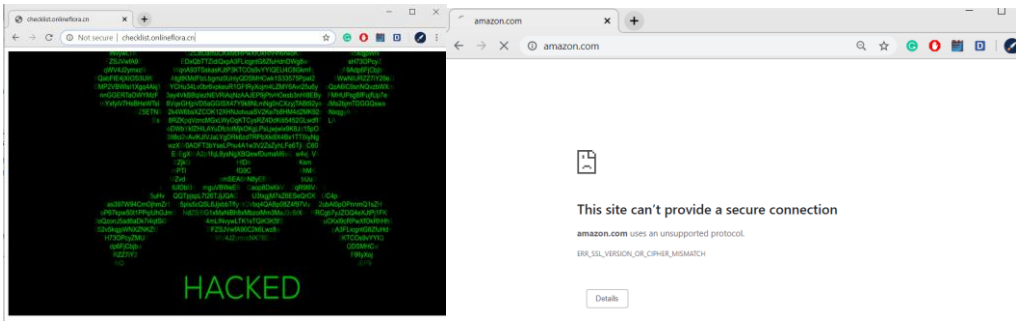


Рис 5. Попытки устройства User получить доступ к интернет ресурсам.

Для защиты от уязвимости ARP рекомендуется организовывать статическое заполнение ARP таблицы на оконечных устройствах, а также осуществлять разделение сети на VLAN. На рисунке 6 представлен фрагмент формирования статической таблицы ARP

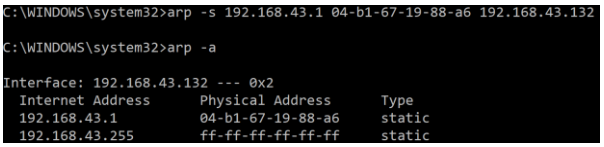


Рис 6. Формирования статической таблицы ARP

Список использованных источников:

Ettrecap manual [Электронный ресурс]. – Режим доступа: https://github.com/Ettercap/ettercap – Дата доступа: 25.03.2020

НЕЙРО-БИОМЕТРИЧЕСКИЕ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Антонюк Е. В.

Хожевец О.А.

Белорусская команда разработала нейро-биометрическую систему управления доступом под названием SVORT, которая очень востребована за пределами Беларуси. Система проверяет реальных пользователей по их лицам. Единственное необходимое оборудование-это веб-камера.

В настоящее время на рынке существует проблема с безопасной аутентификацией. Существует два вида многофакторной аутентификации (MFA). Первый-это OTP (аутентификация через SMS, электронную почту и т. д.), что удобно, но небезопасно. Второй - U2F, который расшифровывается как криптографическая аутентификация с использованием отдельного устройства. Это безопасно, но неудобно. Таким образом, белорусская компания создала нейро-биометрическую систему контроля доступа, которая является более безопаснее, чем первый тип, и более удобная, чем второй. Это система называется SVORT. Система проверяет пользователей по их лицам. Требуется только веб-камера. Принцип работы заключается в том, что нейронная сеть учится преобразовывать сканируемое лицо в статический код, который может использоваться как аутентификатор для предоставления доступа или как закрытый ключ для многофакторных систем аутентификации. Система также защищает пользователей от спуфинговых атак с использованием фотографий, видео и масок. Никакого специального оборудования не требуется. Система может быть интегрирована в любую существующую онлайн-или оффлайн-инфраструктуру безопасности и совместима с любым видом веб-камеры, турникета или электронного замка. Это приложение отличается от FaceID и других приложений тем, что система позволяет пользователям использовать биометрические данные на любом устройстве после регистрации один раз на одном устройстве. Примечательно, что ни ссылки, ни фотография, ни какие-либо другие конфиденциальные данные не хранятся на устройствах или серверах пользователей. Эти разработанные технологии востребованы во многих областях, однако потенциальные клиенты нуждаются в определенных функциях больше, чем сам аутентификатор. Поэтому было решено создать систему, которая будет состоять из 3 основных и 2 дополнительных блоков. Объединив эти блоки, можно будет выполнить любой случай идентификации, аутентификации или верификации. Главной особенностью новой системы является то, что нет необходимости менять существующую инфраструктуру безопасности. Нейронная сеть SVORT учится распознавать лица сотрудников, в то время как они продолжают использовать стандартную систему доступа, постепенно заменяя традиционные ключи.

Разработчик сообщает, что эта система вызвала значительный интерес на ранней стадии: «банки заинтересованы в анонимной биометрической системе, о которой упоминалось выше. Другие заинтересованы в использовании аутентификатора в качестве системы управления доступом. Некоторые впечатлены скоростью системы и предложили использовать ее на турникетах. Компания заключила соглашения по нескольким пилотным проектам с тремя банками из Казахстана и Азербайджана. Сотрудники Национального фонда Казахстана уже проходят в центральный офис по этой системе, а не по карточкам. В 2020 году планируется установить систему на всех 20 этажах фонда.»

Список использованных источников:

1. The neural-biometrics access management system called SVORT[https://dev.by/news/belarusians-working-on-neural-biometrics-access-management-system-raise-usd-200-k-despite-local-business-angels-not-appreciating-the-project].

МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ашурко Д.В.

Власова Г.А. – кандидат техн.наук., доцент

В настоящее время общество переживает самый настоящий информационный бум, и ценность информации нельзя преувеличить. Еще в самом начале 19-го века Натан Ротшильд утверждал, что «тот, кто владеет информацией, владеет миром». И по сей день эти слова не теряют свою актуальность. Информация окружает человека везде, а сфера услуг давно преобладает над сферой товаров, что в очередной раз подтверждает важность информации. Информация дает компаниям по всему миру столь необходимое конкурентное преимущество. Именно поэтому на сегодняшний день существует потребность в повсеместном использовании в организациях систем информационной безопасности. Одним из способов организации информационной безопасности на предприятии является составление моделей нарушителя информационной безопасности.

Модель нарушителя информационной безопасности представляет собой совокупность предположений об одном или нескольких потенциальных нарушителях информационной безопасности, их квалификации, мотивах и т. д. [1] После построения подобной модели можно адекватно оценить систему информационной безопасности организации и выстроить соответствующую систему защиты.

Модель нарушителя строится на основании информации, полученной от службы безопасности организации и аналитических групп, о существующих способах получения несанкционированного доступа к информации, обстановке в коллективе, ситуации в окружающей среде.

Как правило, модель нарушителя является неформальной и отражает мотивы предполагаемых действий, цели, способы и инструменты, используемые для их достижения [2].

Помимо этого, модели нарушителя могут иметь различные степени детализации. Так, например, можно выделить три типа моделей: содержательная, сценарная и математическая. Содержательная отражает систему принятых организацией мер противодействия, сценарная – типы совершаемых действий по классам и этапам, а математическая используется для количественной оценки принимаемых мер и степени защищенности объекта.

Также стоит отметить, что зачастую строится несколько моделей, соответствующих нескольким типам нарушителей информационной безопасности, производится оценка нарушителей по уровням их квалификации и технической оснащенности.

Существует два типа нарушителей: внутренние и внешние.

К внутренним нарушителям можно отнести пользователей системы, администраторов, программистов, специалистов службы безопасности, а также обслуживающий персонал. Среди причин, по которым внутренний нарушитель может прибегнуть к неправомерным действиям можно отметить ошибки, корыстные интересы, безответственность, месть.

В то же время к числу внешних нарушителей можно отнести клиентов организации, конкурентов, сотрудников ведомственных органов.

К методам, используемым нарушителем можно отнести сбор данных, перехват информации, использование недостатков системы и последующее внедрение в нее.

При этом нарушители могут обладать различным уровнем знания о системе: начиная от базовых и вплоть до непосредственного принятия участия в разработке системы.

Что касается места воздействия на систему, то нарушители могут перехватывать информацию удаленно либо при непосредственно физическом контакте с системой.

В результате анализа полученной информации, составляется модель или «портрет» нарушителя. Так, например, можно предположить, что доступ к системе может желать получить группа хакеров, в распоряжении которых имеется локальная вычислительная сеть, которые будут использовать чужие каналы с высокой пропускной способностью с помощью вредоносных программ с целью внесения искажения в работу системы. Или, например, конкуренты, использующие собственные каналы и вычислительные сети, могут предпринять усилия по блокировке функционирования системы, подрыву имиджа и получения секретной информации о функционировании организации.

Таким образом, модель нарушителя информационной безопасности позволяет оценить степень защищенности информационных систем организации от различных способов воздействия на них. Также, с помощью построенных моделей можно предугадать действия различных потенциальных нарушителей, предупредить их и выстроить соответствующим образом систему защиты информационных систем организации.

Список использованных источников:

Модель нарушителя информационной безопасности. [Электронный ресурс] – Режим доступа: https://studfile.net/preview/5443545/page:4/ – Дата доступа: 10.04.2020.

Модель нарушителя информационной безопасности. [Электронный ресурс] – Режим доступа: http://infoprotect.net/varia/modelyy_narushitelya_informacionnoy_bezopasnosti – Дата доступа: 10.04.2020.

Модель нарушителя. [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_%D0%BD%D0%B0%D1%80%D1%83%D1%88%D0%B8%D1%82%D0%B5%D0%BB%D1%8F – Дата доступа: 10.04.2020.

ШИРОКОПОЛОСНЫЙ ПРИЕМНИК РАДИОЛОКАЦИОННОЙ ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ СВЧ ДИАПАЗОНА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Булавко Д.Г., Лисов Д. А.

Гусинский А. В.. – к. т. н., доцент

В докладе рассмотрен широкополосный приемник радиолокационной измерительной системы в диапазоне СВЧ частот. Приведена структурная схема приемника. Рассмотрен способ его построения и особенности его конструкции.

Широкополосный приемник измерительной системы в диапазоне частот 1-18 ГГц предназначен для приема СВЧ излучения, его фильтрации, переноса на промежуточную частоту (ПЧ) с использованием двух ступеней преобразования и усиления сигнала ПЧ перед его поступлением в вычислительный блок. Структурная схема приемника представлена на рисунке 1.

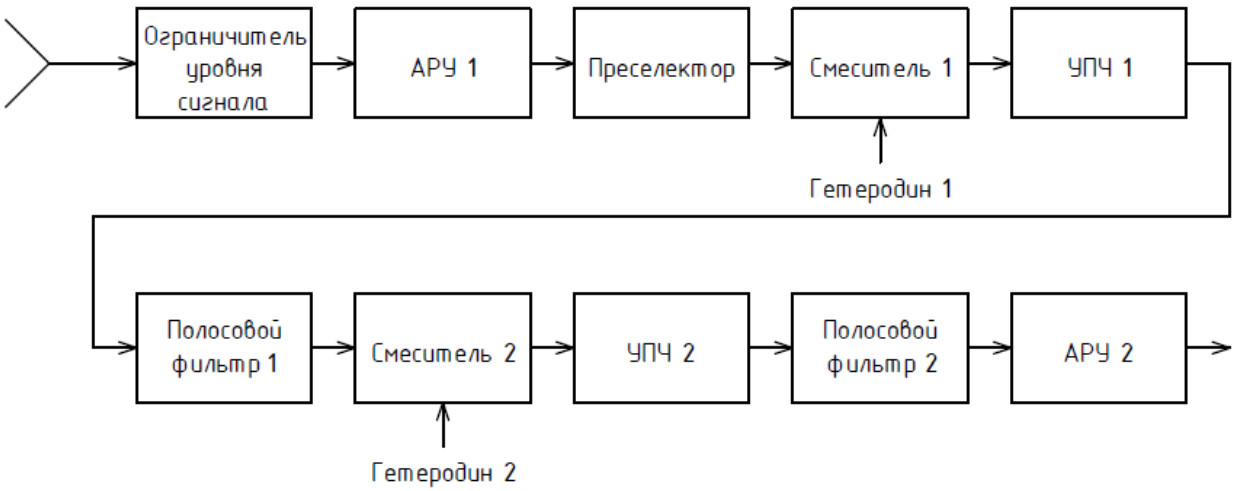


Рисунок 1 – Структурная схема широкополосного приемника измерительной системы

Представленная структура приемника позволяет обеспечить подавление паразитных каналов приема, уменьшить количество фильтров в преселекторе и обеспечивает высокую чувствительность

Ограничитель уровня сигнала обеспечивает защиту входных цепей от высокого уровня принимаемого сигнала. Он рассчитан на максимальную входную мощность сигнала 5 Вт.

Модуль автоматической регулировки усиления 1 (АРУ 1) предназначен для регулирования уровня мощности поступающего на первый смеситель. Состоит из схемы ответвления части мощности сигнала, детектирования уровня и управляемого цифрового аттенюатора.

В преселекторе осуществляется полосовая фильтрация принимаемого сигнала с подавлением внеполосных колебаний не менее 70 дБ. При этом весь диапазон 1-18 ГГц разбит на шесть поддиапазонов 1-2 ГГц, 2-4 ГГц, 4-6 ГГц, 6-11 ГГц, 11-15 ГГц и 15-18 ГГц.

С помощью первого смесителя, первого усилителя промежуточной частоты (УПЧ 1) и полосового фильтра 1 выполняется первое преобразование частоты. Значение частоты ПЧ 1 зависит от выбора обрабатываемого поддиапазона.

Второе преобразование выполняется с помощью смесителя 2, УПЧ 2 и полосового фильтра 2. Значение второй ПЧ составляет 1,25 ГГц, а полоса пропускания второго полосового фильтра равна 500 МГц.

Сигналы первого и второго гетеродинов формируются с помощью внешних синтезаторов частот. Время перестройки синтезаторов составляют десятки микросекунд.

Модуль автоматической регулировки усиления 2 предназначен для регулирования уровня мощности сигнала поступающего на входы аналогово-цифрового преобразователя вычислительного блока. Диапазон регулирования сигнала 45 дБ.

Для уменьшения габаритных и энергетических показателей используются малогабаритные, имеющие минимальные потери фильтры на поверхностно-акустических волнах, усилители с

наименьшими значениями коэффициента шума, многослойные печатные платы и бескорпусные электронные компоненты.

СИСТЕМА ХАНИПОТОВ T-POT

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Грицкевич В.И.

Петров С.Н. – канд. тех. наук

Ханипот (от англ. honeypot, горшочек с медом) – приманка, используемая для привлечения внимания злоумышленников, для которых она может выглядеть, например, как обыкновенный фрагмент компьютерной системы. Ханипоты предоставляют собой средство отвлечения злоумышленников от реальной сети или наблюдения за их деятельностью. Другими словами, ханипот – это сетевая система для определения несанкционированного использования информационной системы путем анализа поведения злоумышленника в изолированной и контролируемой среде. Именно потому, что зачастую невозможно различить легитимный и вредоносный запрос, были созданы такие инструменты, как ханипоты. Ханипот – это информационная система, которая предназначена для мониторинга и обнаружения возможных атак путем имитации уязвимой системы..

Целью создания и использования ханипотов является регистрация всех возможных злонамеренных действий злоумышленника в зависимости от типа ханипота, реализованного в рамках инфраструктуры. Системы ханипот могут использоваться для идентификации различных типов вредоносных действий, такие как атаки веб-приложений, известные эксплуатация уязвимостей, эксплуатация устаревших программ/систем и автоматические атаки вредоносных ботов. Помимо обнаружения различных типов атак, хорошо внедренная система может также использоваться для обнаружения атак эскалации привилегий и их возможных причин. Логика выявления разных атак на повышение привилегий вращается вокруг реализации инфраструктуры с уязвимыми системами и слабыми конфигурациями. Когда злоумышленник использует любую из этих слабых конфигураций или учетные данные из этих намеренно уязвимых систем, ханипот может обнаружить, что злоумышленник скомпрометировал одну из преднамеренно уязвимых систем и пытается произвести атаку повышения привилегий [1].

Среди огромного количества различных ханипотов стоит обратить внимание на такую систему как T-Pot. T-Pot - это коллекция различных ханипотов, собранных компанией T-Mobile. Он представляет реализацию стека ELK (Elastic Search, Logstash, Kibana) для визуализации всех событий, захваченных различными ханипотами и некоторыми другими инструментами.Все ханипоты в T-Pot работают, используя Docker (виртуальный контейнер), что значительно упрощает управление всеми настройками [2].

T-Pot является совокупностью docker-версий следующих ханипотов [3]:

– adbhoney (ханипот слабого взаимодействия для Android Debug Bridg, универсальный интерфейс доступа к устройствам Android с персонального компьютера);

– ciscoasa (ханипот слабого взаимодействия для Cisco ASA, способный обнаруживать CVE-2018-0101, атаки типа отказ в обслуживании и попытки удаленного исполнения команд);

– citrixhoneypot (обнаруживает и логгирует попытки сканирования и эксплуатации CVE-2019-19781);

– conpot (ханипот слабого взаимодействия эмулирующий комплекс инфраструктур, которые заставляют злоумышленника подумать, что он обнаружил большой промышленный комплес);

– cowrie (SSH и Telnet ханипот среднего взаимодействия, логгирующий брутфорс-атаки и команды, выполняемые злоумышленником);

– dionaea (сборник ханипотов, работающий на таких протоколах, как http, ftp, mysql и т.д.);

– elasticpot (ханипот Elastic Search);

– glutton (работает как MITM между злоумышленником и сервером, логгируя все действия);

– heralding (собирает авторизационные данные с протоколов ssh, telnet, ftp, rdp, http, https, pop3, pop3s, imap, imaps, smtp, vnc, postgresql, socks5);

– honeypy (плагины, эмулирующие UDP и TCP сервисы);

– honeytrap (динамически запускает серверные процессы на портах, к которым происходит обращение);

– mailoney (SMTP ханипот);

– rdpy (ханипот удаленного рабочего стола);

– snare+tanner (веб-ханипот).

Далее представлены результаты работы системы T-Pot за декабрь 2019 года.

Наибольшее количество атак пришлось на следующие модули системы T-Pot:

– dionaea (20843332 атаки, большая часть из которых пришлась на модуль эмулирующий SQL-сервер);

– honeytrap (716538);

– heralding (233784);

– rdpy (169583);
– mailoney (23765).

Если рассматривать статистику со всей системы T-Pot, то наиболее активными странами с точки зрения количества попыток несанкционированного доступа являются:

– Российская Федерация (4619164);
– Индия (1907802);
– Вьетнам (1402678);
– Армения (1050582);
– Индонезия (953348).

Если же рассматривать статистику несанкционированных попыток доступа к веб-серверу, то ситуация нескол

– Китай (3497);
– Гонгконг (865);
– США (574);
– Италия (473);
– Франция (321).

Безусловно, эти данные не отражают реальной картины, так как подавляющее большинство злоумышленников используют средства анонимизации в сети Интернет, однако их можно использовать для составления общей картины в целом.

Помимо этого, были собраны данные по наиболее часто используемым именам пользователей (рисунок 1) и паролям (рисунок 2).

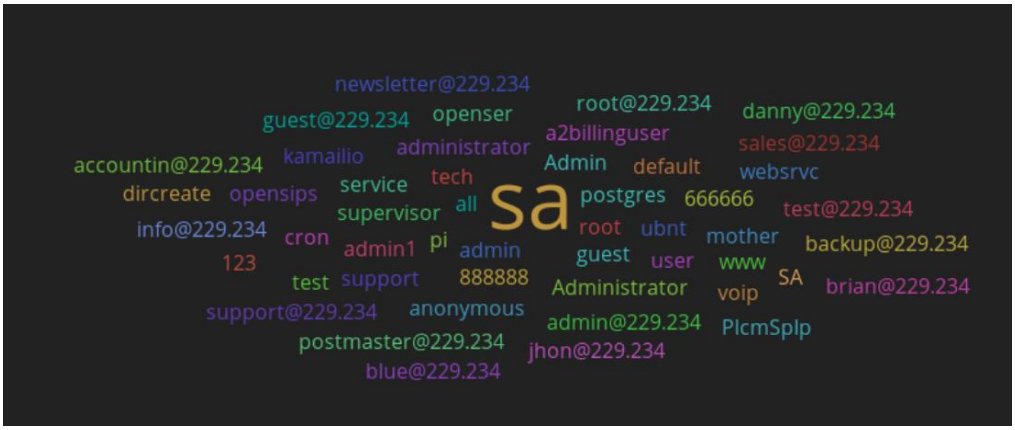


Рисунок 1 – Наиболее часто используемые имена пользователей

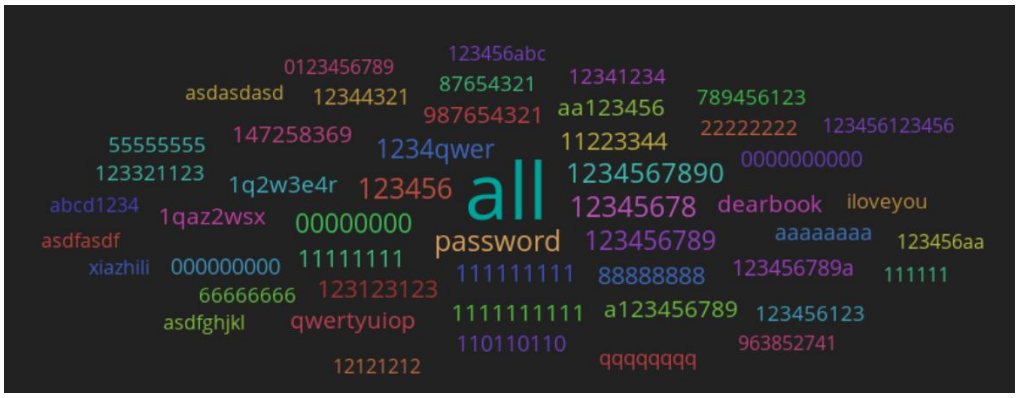


Рисунок 2 – Наиболее часто используемые пароли

Таким образом, можно сделать вывод о том, что ханипоты предоставляют информацию, которую можно использовать для анализа активности потенциальных злоумышленников, и с учетом этого повышать уровень защищенности информационных систем..

Список использованных источников:

1. Ханипот (Honeypot) [Электронный ресурс]. – Режим доступа: https://encyclopedia.kaspersky.ru/glossary/honeypot/.
2. Introduction to T-Pot - The all in one honeypot [Электронный ресурс]. – Режим доступа: https://northsec.tech/introduction-to-t-pot-the-all-in-one-honeypot/.
3. Концепция системы T-Pot [Электронный ресурс]. – Режим доступа: https://github.com/dtag-dev-sec/tpotce#concept.

МЕТОДИКА ОЦЕНКИ ЗАЩИЩЕННОСТИ ВЕБ-РЕСУРСОВ НА БАЗЕ МЕТРИКИ CVSS

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Давлатов Ш.Р.

Кучинский П.В. – доктор физико-математических наук

В рамках данной работы была создана система для сбора технической информации об активных веб-ресурсах в сети интернет из общедоступных каталогов и реестров. На основе анализа данных об уязвимостях веб-ресурсов и метрики CVSS определяется распределение усредненной величины оценки уязвимости для каждого ресурса. Разработаны шаблоны поиска с помощью RegExp выражений языка JavaScript для точного определения версий технологий, которые были использованы для создания веб-сайтов. На базе полученных данных установлены процентные соотношения используемых технологий, доменов верхнего уровня и географическое расположение серверов, которые обслуживают веб-ресурсы. Данная разработка была апробирована на примере 19 тысяч наиболее популярных веб-ресурсов Беларуси.

С развитием веб-технологий растет и число потенциальных уязвимостей в онлайн-ресурсах. Широкое использование инструментов для реализации угроз информационной безопасности в Интернете определяет актуальность использования систем для анализа безопасности веб-ресурсов. Специалисты по защите информации широко используют объективные количественные показатели защищенности, которые вычисляются на основе метрик открытой системы оценки CVSS [1] (Common Vulnerability Scoring System). Существуют открытые базы данных, где хранится информация об уязвимостях определенных версий технологий в формате <название технологии, версия, оценка CVSS>. Метрика CVSS предлагает простой инструментарий для расчета числового показателя уязвимости по десятибалльной шкале [2]. Чем выше значение метрики, тем более оперативная реакция требуется для исправления проблемы безопасности системы.

В рамках данной работы были разработаны NodeJS скрипты для автоматического сбора информации о веб-ресурсах из открытых источников shodan.io и censys.io. В результате процесса сканирования удалось собрать данные более 19 тысяч веб-ресурсов Беларуси, которые были разделены на 5 категорий. Для каждого отдельного домена была получена техническая информация в формате: IP-адреса, открытые порты, географическое расположение веб-серверов и заголовки ответов HTTP. Далее, с помощью RegExp выражений языка JavaScript определяются версии технологий, на базе которых были созданы веб-ресурсы. Для решения поставленной задачи достаточно получить исходный код страницы веб-сайта в формате HTML и заголовки ответов сервера [3]. Результаты запросов и заголовки ответов сервера были сохранены в локальной базе данных для последующих процессов обработки и анализа данных. Данный скрипт также может обнаруживать типы систем управления контентом (CMS), платформы электронной коммерции, версии веб-фреймворков, серверное программное обеспечение и аналитические инструменты. Последним этапом является проверка безопасности каждого веб-ресурса по отдельности на базе публичных API.

На основе полученных данных о версиях технологий была создана диаграмма, показывающая процентное соотношение используемых технологий для разработки веб-ресурсов в шести категориях (рис. 1).

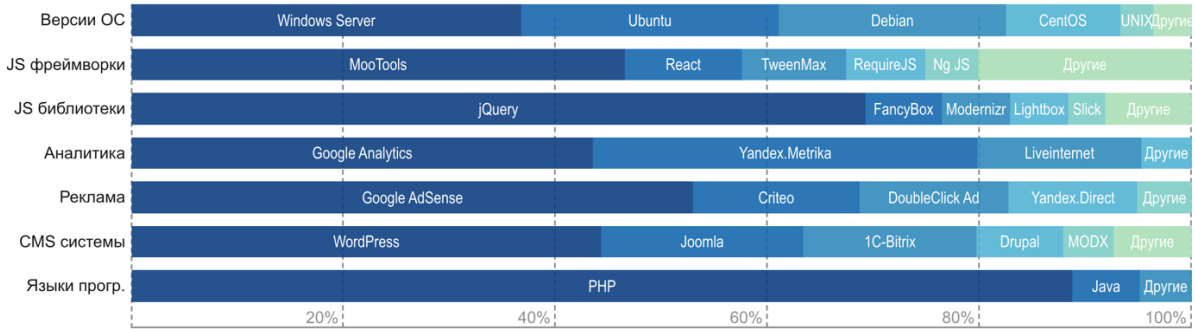


Рисунок 1 – Процентное соотношение используемых технологий в веб-ресурсах

Данные о географических расположениях серверов, обслуживающие веб-ресурсы из нашей исходной выборки, представлены в виде наглядной столбчатой диаграммы (рис. 2). На оси X расположены названия стран, где сосредоточено наибольшее количество веб-серверов: Беларусь, Россия, США, Германия и другие страны (Нидерланды, Польша, Украина и Великобритания).

Каждый столбец показывает количество серверов, которые обслуживают веб-ресурсы определенной категории в той или иной стране.

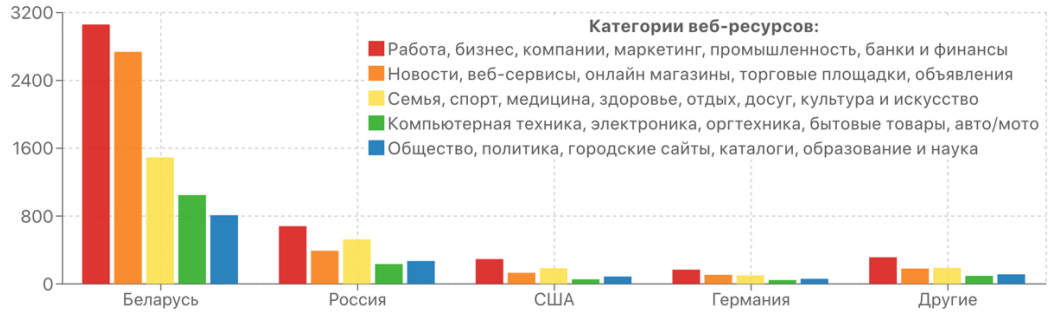


Рисунок 2 – Распределение веб-ресурсов по категориям и странам расположения серверов

Процентное соотношение доменов верхнего уровня показаны на рисунке 3 в виде круговой диаграммы. Данные были получены из исходной выборки веб-ресурсов путем приведения доменных имен к каноническому виду. Из рисунка видно, что домены BY составляют примерно 75% из всех имеющихся записей в базе данных. А в свою очередь домены COM и RU составляют 8,8% и 8,2% соответственно. Следует отметить, что все остальные домены (NET, БЕЛ, ORG и другие) были объединены в одну категорию с процентной долей 7,5%.

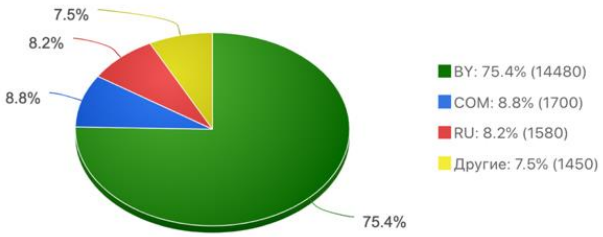


Рисунок 3 – Процентное соотношение доменов верхнего уровня

В рамках данного исследования также был проведен анализ оценки уязвимостей всех веб-ресурсов из нашей исходной выборки. Для каждого веб-ресурса была использована усредненная оценка CVSS в соответствии с выражением $Si = (A1+A2+\ldots+Am)/m$, $1 \le i \le n$, где n – количество элементов в нашей выборке; m – количество распознанных версий технологий и ЯП для заданного веб-ресурса; Aj – оценка уязвимости определенной версии технологии. Для вычисления значения Aj была выбрана функция максимума по всем известным оценкам CVSS: $Aj = \max(Ck)$, $1 \le k \le r$, где r – количество найденных уязвимостей для определенной версии технологии в общедоступной базе vulners.com. Для исследования распределения была создана случайная выборка из исходной базы данных веб-ресурсов, состоящая из N = 2000 элементов (около 10% записей). На основе этих данных была построена диаграмма эмпирического распределения усредненной оценки уязвимости Si веб-ресурсов (рис. 4).

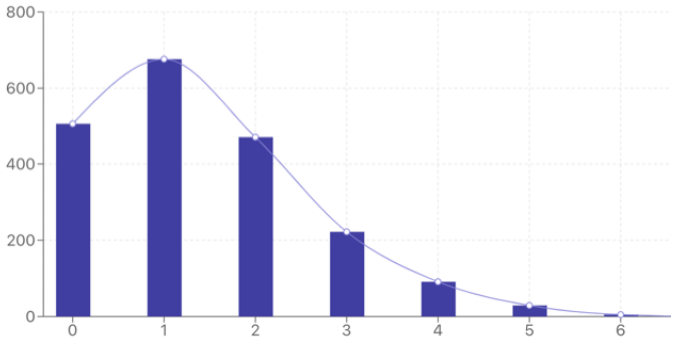


Рисунок 4 – Диаграмма эмпирического распределения оценок уязвимостей веб-ресурсов

Следует отметить, что в исходной генеральной совокупности, порядка 90% веб-ресурсов имеют значение усредненной оценки CVSS в интервале [0, 5]. Было выявлено, что остальные 10% ресурсов имеют высокую критическую оценку уязвимости из-за использования устаревших версий таких технологий как: CMS WordPress, ЯП PHP, веб-сервера nginx и JavaScript библиотеки jQuery.

Список использованных источников:

1. Дойникова, Е. В., Чечулин, А. А., Котенко, И. В. Оценка защищенности компьютерных сетей на основе метрик CVSS // Информационно-управляющие системы, 76-87. DOI: 10.15217/issn1684-8853.2017.6.76.

2. Li, H., Zhao, L. Study on the distribution of CVSS environmental score // 5th International Conference on Electronics Information and Emergency Communication. May 2015. DOI: 10.1109/ICEIEC.2015.7284502.

3. Bostic, T., Stanley J., Higgins, J., Chudnov, D., Montgomery, B., Brunell, J. Exploring the Intersections of Web Science and Accessibility // The MITRE Corporation Scientific journal. Aug 2019.

УГРОЗЫ БЕЗОПАСНОСТИ И СПОСОБЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТА ПРИ ОСУЩЕСТВЛЕНИИ QR ПЛАТЕЖЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Боложко П.А., Игнатчик Д.С.

Белоусова Е.С. – канд. техн. наук, доцент

Использование QR-кодов в повседневной жизни облегчают пользователям доступ к данным с помощью любого современного устройства с камерой. При этом возникают вопросы обнаружения уязвимостей использования QR-кодов, а также обеспечения безопасности транзакций.

Суть технологии QR (Quick Response Code) заключается в ее совместимости с сервисом SmartPay, которое может быть, как банковским, так и коммерческим. Установив приложение на устройство и осуществив выбор товаров, покупатель может оплатить их QR-платежом. После открытия приложения и получения уникального QR-кода устройство необходимо приложить к сканеру, и оплата будет реализована. В приложение покупатель получит электронный чек. Проблема в том, что отличить QR-код магазина от QR-кода злоумышленника на глаз невозможно. Если торговая точка использует статический код, киберпреступник может просто заклеить его своим. Для этого ему необходимо создать QR-код с личным счетом, используя приложения-генераторы, которые находятся в открытом бесплатном доступе.

На основе проведенных исследований нами предложено два основных типа возможных мер по нейтрализации угроз при осуществлении QR-платежей: социально-психологические меры и инженерно-технические, основанные на использовании специального программного обеспечении (ПО).

В качестве социально-психологических мер предлагаются следующие:

– проверка суммы оплаты и ее получателя перед подтверждением транзакции;

– проверка легитимности код (не наклеен ли он поверх другого);

– генерирация платёжного кода непосредственно в момент оплаты.

В качестве специального ПО мы факультативно разрабатываем программу «предаутентицификации продавца», принцип которой основан на использовании стандарта EMVCo для платежей с помощью QR (рисунок 1).

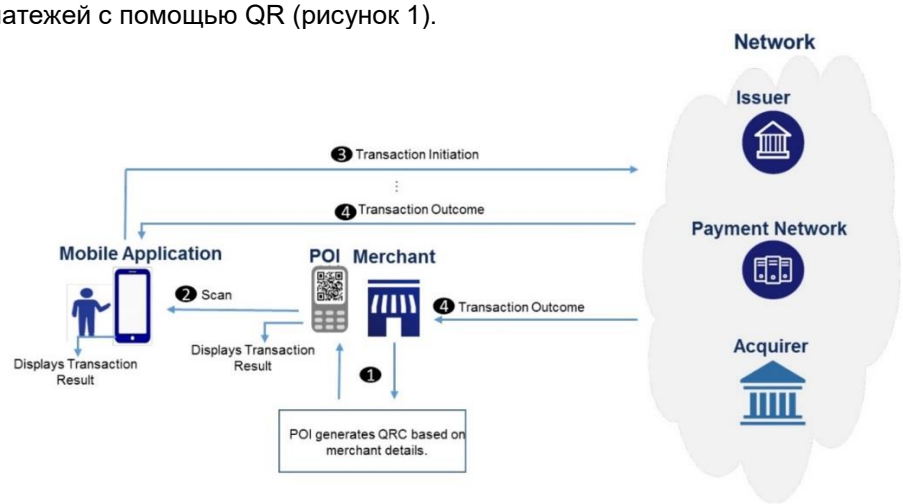


Рисунок 1 – Стандарт EMVCo для QR-платежей

После сканирования данных информация о транзакции дублируется и передаётся на выделенный сервер, где проходит обработку и сопоставляется с открытой банковской базой данных юридических лиц. В случае успешного сравнения и получения одобрения от сервера копия информации о транзакции идёт далее по представленной на рисунке 1 схеме. В случае неодобрения транзакция прерывается и информация отправляется в FINCert Национального Банка Республики Беларусь. Таким образом, правильная и эффективная работа данной системы возможна только при консолидации всех субъектов банковской сферы Республики Беларусь.

Список использованных источников:
Оплата по QR коду - https://www.raschet.by/platelshchikam/ais-raschet/oplata-po-qr-kodu/
Опыт Китая по созданию расчетного пространства и оплате QR-кодами - https://www.hutkigrosh.by/blog/oplataqrkodami/
QR-коды — от Японии до России - https://www.kaspersky.ru/blog/qr-code-payments/22960/

БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ: КОММУНИКАЦИОННЫЕ АСПЕКТЫ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кадушко А.А.

Филатова Д.В. – д.ф.-м.н

В работе рассмотрена концепция фабрики будущего. Показано, что основной проблемой распространения технологии фабрики будущего является кибербезопасность, описана система связи устройство-устройство (D2D). Рассмотрена классификация существующих архитектур систем связи устройства-к-устройству киберфизические систем, а также методов защиты информации.

Концепции фабрики будущего основаны на нескольких принципах: открытость цепочки создания стоимости (понимаемая как адекватность, гибкость, устойчивость и оптимальность по отношению к капитальным затратам, связанных с планированием и управлением предприятием), гибкость производства (по объему, продукту, дизайну, процессу и автоматизации), клиент-ориентированное производство, специфика бизнес-модели (краудсорсинг, AaaS-принцип, симбиотическая экосистема), локальная инициатива («smart»-производство, промышленный интернет, электронная фабрика, Industry 4.0, интеллектуальное производство) [1]. Попытка обобщения концепций привела к появлению понятия «RAMI 4.0», т.е. «модель эталонной архитектуры» [2]. Архитектура отображает фабрику будущего с использованием трехмерной классификации: управление фабрикой - «Layers», иерархия оборудования, материальных и нематериальных ресурсов – «Levels», поток создания стоимости при жизненном цикле – «Life Cycle Value Stream». Отличительной чертой такого восприятия является появление «физической» и «информационной» систем-оболочек, причем вторая воспринимается как клон первой и используется для управления фабрикой в целом [2, 3].

Осуществление управления при помощи информационной оболочки зависит от выбора платформы и ее архитектуры. Одним из решений является архитектура с использованием CPMT (от англ. «cyber-physical machine tools» – киберфизические станки). Идея заключается в представлении CPMT в виде трех подсистем: физические устройства (physical devices), сети (networks) и цифрового близнеца физических устройств, содержащего также алгоритмы обработки информации, диагностики и управления. Очевидно, что между физическими устройствами и их информационными близнецами постоянно происходит передача данных, которые по скорости, объему и структуре характеризуются как Big Data. Но, несмотря на прогресс в области информационных технологий, существуют барьеры, ограничивающие распространение такого решения: связь и взаимодействие физических и информационных уровней предприятия, архитектура системной интеграции, охрана и безопасность хранения и передачи информации между уровнями. Поэтому среди перспективных направлений исследований являются: интернет вещей (IoT) и межмашинное общение (M2M, D2D), облачная инфраструктура приложений и промежуточное ПО, аналитика данных (вычисления в базе данных в памяти, обработка потоков событий, комплексная обработка событий, механизмы принятия решений), умная робототехника (взаимодействие человека и робота, новые парадигмы программирования роботов), интегрированное моделирование производства продукции, аддитивное производство / 3D печать.

Использование интернета вещей связано с проблемой загруженности сети (использование системы связи, построенной на использовании базовых станций, неэффективно, хотя бы из-за отсутствия возможности поддержки неограниченного количество устройств в своей сети без потери качества связи). Альтернативой является 5G технология, т.е. система связи устройство-к-устройству без использования базовых станций [4]. Главная проблема этой технологии - отсутствие формализованных стандартов и методов защиты чувствительных данных. Целью этой работы является изучение и классификация существующих архитектур систем связи устройства-к-устройству киберфизические систем, а также методов защиты информации.

Список использованных источников:

1. Kagermann, H. Securing the future of German manufacturing industry: recommendations for implementing the strategic initiative INDUSTRIE 4.0 / Kagermann H., Wahlster W., Helbig J. // Final report of the Industrie 4.0 Working Group - 2013. – vol. 40, pp. 1 – 84.
2. Lee, J. A cyber-physical systems architecture for industry 4.0-based manufacturing systems / J. Lee, B. Bagheri, H.A. Kao // Manufacturing Letters – January 2015 – vol.3, pp. 18 – 23.
3. Filatova, D. Production process balancing: a two-level optimization approach / D. Filatova, Ch. El-Nouty // International Conference on Information and Digital Technologies (IDT) 2019, – IEEE, 2019 – pp. 123-131.

4. Haus M. Security and Privacy in Device-to-Device (D2D) Communication: A Review / M. Haus, Wagas M., Ding A.Y., Li Y., Tarkoma S., Ott J. // IEEE Communications Surveys & Tutorials, 2017, - IEEE, vol.19 (2) - pp. 1054 - 1079.

ПРАКТИКИ МИНИМИЗАЦИИ ИНФОРМАЦИОННЫХ РИСКОВ В ОРГАНИЗАЦИЯХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Казберович И.Г.

Власова Г.А. – канд. техн. наук, доцент

В современном мире бурно развиваются технологии обработки, хранения и передачи информации. Применение информационных технологий требует повышенного внимания к вопросам информационной безопасности. Риск информационной безопасности организации представляет собой возможный ущерб организации в результате реализации некоторой угрозы через уязвимость. Нарушение информационной безопасности организации влечет уничтожение информационных ресурсов, недоступность либо их несанкционированное использование, что нарушает “непрерывность” бизнеса, приводит к финансовым потерям и ущербу репутации.

Для обеспечения информационной безопасности малых и средний компаний предложены следующие практики:

1. Разграничение доступа сотрудников через аутентификацию пользователей и межсетевые экраны.
2. Симуляция “фишинговых” атак для тренировки и подготовки сотрудников к подобным случаям. Согласно исследованиям компании “PhoenixNap” в 2020 году, данные атаки являются наиболее популярными среди компаний на мировом уровне.
3. Реализация удаленного доступа к корпоративной сети через VPN и использование антивирусных программ позволяют уменьшить риски атак в случае удаленной работы сотрудников.
4. Осведомленность сотрудников, удаленных сотрудников и аутсорсинговых сотрудников о конфиденциальности данных организации и их собственных данных, политиках безопасности и государственных законах путем проведения “воркшопов”, тренингов и презентаций. Согласно исследованиям Ponemon Institute, 2 из 3 атак инициируются сотрудниками и могут быть предотвращены.
5. Избежание методов социальной инженерии через sms, email, звонки, профили социальных сетей и т.д. с помощью которых получают авторизационные данные сотрудников и доступ к защищенным файлам. Сотрудники должны быть осведомлены о возможности подобных атак.
6. Внедрение подхода по управлению рисками информационной безопасности, что позволит сотрудникам оперативно определять, исследовать и реагировать на инциденты.
7. Покупка/разработка программного обеспечения по мониторингу пользовательской и файловой активности. Мониторинг пользователей позволяет легче реагировать и предотвращать инциденты.
8. Необходимо использовать менеджеры паролей (LastPass, Dashlane, CommonKey и т.д.). Использование слабых либо повторяющихся паролей одна из самых распространенных практик.
9. Периодический пересмотр списка сотрудников (особенно при увольнениях либо переходах сотрудников), имеющих привилегированный доступ к важным областям бизнеса/данным, либо разработка системы аудита привилегированных доступов.
10. Резервное копирование данных на регулярной основе.
11. Регулярные обновления и обслуживание используемых систем и обеспечения.
12. Поддержание в актуальном состоянии планов обработки рисков (информационных активов, каталогов угроз и уязвимостей и т.д.).
13. Поддержание процессов информационной безопасности в соответствии стандартам ISO, PCI, DSS, HIPAA. [1,3]

Согласно исследованиям компании “Positive Technologies” в 2019 году, из 33 организаций, протестированных на внутреннее и внешнее проникновение, популярными уязвимостями являются недостатки парольной политики, эксплуатация недостатков защиты беспроводных сетей, применение социальной инженерии и, следовательно, низкий уровень осведомленности пользователей в вопросах информационной безопасности. В результате внешнего тестирования на проникновение в 92% из 33 исследуемых компаний удалось преодолеть сетевой периметр по причине проблемы несвоевременного обновления программного обеспечения (версии прикладного ПО, серверов, веб-приложений). В результате внутренних тестов на проникновение в 100% исследуемых компаний получен контроль над внутренней инфраструктурой по причине недостаточного уровня защиты привилегированных учетных записей, словарных паролей, недостатков защиты служебных протоколов сети и хранения важной информации в открытом виде.

Для минимизации информационных рисков в организации важно следовать всем рекомендациям в комплексе, так как даже отдельные пробелы в механизмах защиты могут послужить причиной взлома инфраструктуры и компрометации критически важных ресурсов. [2]

Список использованных источников:

Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Проверка и оценка деятельности по управлению информационной безопасностью: научное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой — М.: Горячая линия-Телеком, 2013. — 166 с.

Официальный сайт компании “Positive Technologies” [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/ - Дата доступа: 04.04.2020.

Официальный сайт компании “phoenixNAP” [Электронный ресурс]. – Режим доступа: https://phoenixnap.com/blog/cybersecurity-best-practices - Дата доступа: 07.04.2020.

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ В КОРПОРАТИВНЫХ СЕТЯХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Климов Д.А.

Ширинский В.П. – к.т.н.,доцент

Изложена классификация угроз корпоративным сетям по различным аспектам, подходы к защите информационных систем, политики безопасности предприятия.

Трудности решения практических задач обеспечения безопасности конкретных операционных систем связаны с отсутствием развитой стройной теории и необходимых научно-технических и методических основ обеспечения защиты информации в современных условиях.

Уязвимыми являются буквально все основные структурно-функциональные элементы современных ОС. Защищать компоненты ОС необходимо от всех видов воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, ошибок в программах и от преднамеренных действий злоумышленников.

Угрозы безопасности операционной системы существенно зависят от условий ее эксплуатации, от того, какая информация в ней хранится и обрабатывается, и т. д.

Угрозы безопасности операционной системы можно классифицировать по различным аспектам их реализации:

- по цели атаки;
- по принципу воздействия на операционную систему;
- по типу используемой злоумышленником уязвимости защиты;
- по характеру воздействия на операционную систему.

Вышеперечисленные типы угроз и проникновений могут вызывать множество видов проблем различных уровней – от относительно безобидных до представляющих крайне серьезную степень опасности. Тем не менее, даже кажущиеся несерьезными нарушения могут в итоге приводить к существенному нарушению работы корпоративных сетей. Именно поэтому в современном мире необходимо осуществлять постоянный пересмотр и обновление подходов к защите операционных систем.

Существует два основных подхода к созданию защищенных операционных систем – фрагментарный и комплексный. При фрагментарном подходе вначале организуется защита от одной угрозы, затем от другой и т. д. Примером, фрагментарного подхода может служить ситуация, когда за основу берется незащищенная операционная система, на нее устанавливают антивирусный пакет, систему шифрования, систему регистрации действий пользователей и т. д.

При применении фрагментарного подхода подсистема защиты ОС представляет собой набор разрозненных программных продуктов, как правило, от разных производителей. Эти программные средства работают независимо друг, от друга, при этом практически невозможно организовать их тесное взаимодействие. Кроме того, отдельные элементы такой подсистемы защиты могут некорректно работать в присутствии друг друга, что приводит к резкому снижению надежности системы.

Программно-аппаратные средства защиты операционной системы обязательно должны дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже надежная программно-аппаратная защита может давать сбои [1].

Политика безопасности подразумевает наличие множества условий, при которых пользователи системы могут получить доступ к информации и ресурсам. С одной стороны, политика безопасности предписывает пользователям, как правильно эксплуатировать систему, с другой – она определяет множество механизмов безопасности, которые должны существовать в конкретной реализации ОС. Политика безопасности ОС может быть выражена формальным и неформальным образом. Выбор и поддержание адекватной политики безопасности являются одной из наиболее важных задач администратора операционной системы.

Таким образом, политика безопасности должна учитывать два главных фактора:

- максимальную защиту операционных систем от внешних и внутренних, санкционированных и несанкционированных вторжений;

- в то же время доступность и отзывчивость для администраторов и пользователей самой корпоративной сети [2].

Список использованных источников:

1. *Шаньгин В.Ф. Комплексная защита информации КС. Эффективные методы и средства [Электронный ресурс] : [учебное пособие] / В.Ф. Шаньгин – М : ДМК-Пресс, 2010. – 545с.*
2. *Проскурин В.Г., Защита в операционных системах: Учебное пособие для вузов / Проскурин В.Г. – М. : Горячая линия – Телеком,2014. – 192с.*

НАДЕЖНОСТЬ СИСТЕМ КОНФИДЕНЦИАЛЬНОЙ СВЯЗИ, ОРГАНИЗОВАННОЙ ПО ВОЛОКОННО-ОПТИЧЕСКИМ КАНАЛАМ

Тимофеев А. М., Колядич А. С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Тимофеев А. М. - кандидат технических наук, доцент

Обеспечение конфиденциальности передаваемой информации – одна из наиболее важных задач при разработке современных систем связи. Решение этой задачи возможно посредством систем квантово-криптографической связи, перспективность использования которых обусловлена возможностью достижения абсолютной конфиденциальности передаваемых данных, это достигается за счет применения маломощных оптических сигналов и, соответственно, высокочувствительных приемных модулей — счетчиков фотонов [1, 2]. При этом важно учитывать, что приемное оборудование (счетчики фотонов) обеспечивало наименьшие потери передаваемой информации. Мертвое время счетчиков фотонов – это время, в течение которого счетчик фотонов не чувствителен к падающему на него оптическому излучению [2]. Целью данной работы являлось определение влияния мертвого времени счетчика фотонов на потери передаваемой информации в квантово-криптографическом канале связи, в котором данные представляют собой последовательности двоичных символов «0» и «1». Объект исследования – асинхронный квантово-криптографический канал связи [3], который не требует наличия линий связи для передачи и приема синхроимпульсов. Предмет исследования – установление влияния продлевающегося мертвого времени типа на энтропию потерь. Данным типом мертвого времени характеризуются счетчики фотонов на базе лавинных фотоприемников, включенные по схеме пассивного гашения лавины [1]. На рис. 1 представлены зависимости энтропии потерь от средней длительности мертвого времени продлевающегося типа для различных средних скоростей счета сигнальных импульсов при передаче символов «0» n_{s0} и символов «1» n_{s1}.

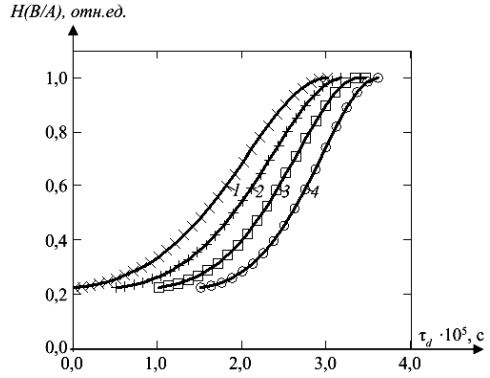


Рисунок 1 – Зависимость энтропии потерь от средней длительности мертвого времени

Выполненные исследования показали, что с ростом средней длительности мертвого времени продлевающегося типа энтропия потерь увеличивается. Причем при прочих равных параметрах с ростом средних скоростей счета сигнальных импульсов при передаче символов «0» и символов «1» энтропия потерь уменьшается.

Список использованных источников:

1. Квантовая криптография: идеи и практика / С.Я. Килин. Минск: Белорус. наука, 2007.

2. Тимофеев А.М. Устройство для передачи и приема двоичных данных по волоконно- оптическому каналу связи // Приборы и методы измерений. 2018.

3. Тимофеев А.М. Оценка влияния продлевающегося мертвого времени счетчика фотонов на вероятность ошибочной регистрации данных квантово-криптографических каналов связи / А.М. Тимофеев // Вестник связи. – 2018.

СВЕРХШИРОКОПОЛОСНЫЙ ГЕНЕРАТОР СЛОЖНЫХ СИГНАЛОВ МИКРОВОЛНОВОГО ДИАПАЗОНА

Лисов Д.А., Булавко Д.Г.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гусинский А.В. – канд. техн. наук

В докладе рассматривается структурная схема сверхширокополосного генератора сложных сигналов. Этот генератор предназначен для проведения антенных измерений и исследований параметров радаров во всём микроволновом диапазоне.

В настоящее время приобретает актуальность задача формирования сложных радиотехнических сигналов в диапазоне частот от 2 до 298 ГГц для осуществления антенных измерений и исследований параметров радаров. В этих целях традиционно используют стандартное измерительное оборудование [1]: векторной генератор с переносчиком частоты, позволяющее обеспечить формирование сложных радиотехнических сигналов до 40 ГГц.

В докладе рассматривается схема (рис.1) сверхширокополосного генератора сложных сигналов, позволяющего перекрыть весь микроволновый диапазон от 2 до 298 ГГц. С целью расширения частотного диапазона были использованы в переносчиках частоты смесители, а не умножители частоты. Кроме того, при построении генератора была предусмотрена возможность использования сменных модулей переносчиков частоты и сменных антенных модулей. Частота сигнала, излучаемого в пространство, разбивается на поддиапазоны, которые зависят от комбинации сменных модулей: антенного и переносчика частоты, размещённых во втором блоке генератора.

Первый блок генератора отвечает за генерацию сигналов в аналоговом виде с частотой гетеродина ЧГ1, второй блок обеспечивает формирование сигналов в диапазоне частот 2-298 ГГц.

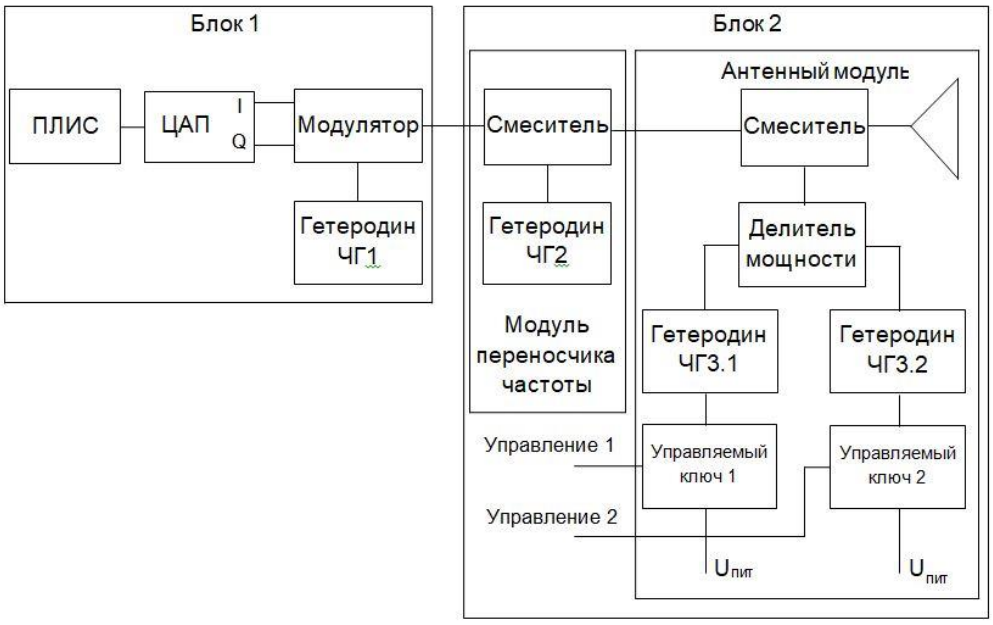


Рисунок 1 – Структурная схема сверхширокополосного генератора сложных сигналов

С помощью ПЛИС и ЦАП блока 1 формируется модулирующий сигнал с заданными параметрами частоты, амплитуды и фазы. Промодулированный сигнал первого гетеродина подаётся на смеситель переносчика частоты блока 2 и далее на антенный модуль.

Список использованных источников:

1. E8267D PSG Vector Signal Generator. Data Sheet [Электронный ресурс]. – Режим доступа: https://www.keysight.com/main/gated.jspx?lb=1&gatedId=473817&cc=BY&lc=eng&parentContId=x202238&parentContType=pt&parentNid=-32488.1150404&fileType=VIEWABLE

СОЗДАНИЕ СТРАТЕГИИ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Любчик Д.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пулко Т.А. – канд. тех. наук, доцент

Каждый день в информационных системах обнаруживается множество новых уязвимостей, причем обнаруживаются они как с целью их исправления, так и для их эксплуатации. Исправляются уязвимости часто после обнаружения факта их использования. К моменту исправления, общий ущерб от эксплуатации уязвимости является значительным. Это обязывает к созданию процесса управления уязвимостями, который можно использовать для их выявления и нейтрализации.

Оптимальный подход к созданию эффективной стратегии управления уязвимостями - сделать ее жизненным циклом управления уязвимостями. Как и жизненный цикл атаки, жизненный цикл управления уязвимостями упорядочено планирует все процессы по их нейтрализации. Это позволяет целям и жертвам инцидентов, связанных с кибербезопасностью, нейтрализовать ущерб, который они понесли [1].

Стратегия управления уязвимостями состоит из шести отдельных этапов. Первым этапом в стратегии управления уязвимостями должно быть проведение инвентаризации активов. Но во многих организациях отсутствует либо содержится не полный реестр активов, поэтому они испытывают трудности при защите своих устройств. При создании стратегии управления уязвимостями, организация должна начать с того, чтобы сделать одного из сотрудников ответственным за инвентаризацию активов с целью гарантировать, что все устройства зарегистрированы и что результат инвентаризации всегда актуален [2]. Без этого о некоторых устройствах можно забыть при исправлении или установке нового программного оборудования, используемого для обеспечения безопасности. Это устройства и системы, на которые будут нацелены злоумышленники. Организациям также не хватает эффективных инструментов, чтобы поддерживать инвентаризацию в согласованном порядке. Обновленный реестр активов пригодится, когда организации придется реагировать на уязвимости, исправляя все свои ресурсы.

Вторым этапом стратегии управления уязвимостями является управление информацией, т.е. контроль того, как информация поступает в организацию. Наиболее важной информацией является интернет-трафик, поступающий из сети организации. Кроме того, организации хранят различные типы данных, и некоторые их них ни в коем случае не должны попасть в руки злоумышленников. Если к коммерческой тайне и личной информации клиентов получат доступ хакеры. это может нанести непоправимый ущерб. Организация может лишиться своей репутации и потерять клиентов. Следовательно, управление информацией имеет жизненно важное значение в стратегии управления уязвимостями. На данном этапе также должно стать создание эффективного способа передачи информации об уязвимостях и инцидентах в области кибербезопасности соответствующим лицам в кротчайшие сроки. На этом этапе существует несколько проблем. Одна из проблем в том, что с годами объемы информации в организации постоянно увеличивается, что усложняет работу с ней, а также контроль над доступом к ней. Ценная информация, касающаяся взломов, такая как оповещения, также может превышать возможности обработки большинства IT-отделов. Релевантные оповещения об атаках могут отбрасываться как ложные срабатывания из-за количества аналогичных оповещение, которые возникают ежедневно. Также возникает проблема, когда речь идет о передаче информации о новых уязвимостях обычным пользователям, которые не разбираются в технических особенностях. Все это влияет на время отклика и действия, которые организация может предпринять в случае потенциальных или проверенных попытках взлома.

Оценка рисков является третьим этапом в стратегии управления уязвимостями. Прежде чем риски могут быть уменьшены, требуется проведение углубленного анализа уязвимостей. В идеальных условиях сотрудники по обеспечению безопасности в организации могут реагировать на все уязвимости, поскольку у нее достаточно ресурсов и времени. Однако в действительности существует очень много ограничивающих факторов. Вот почему оценка рисков имеет решающее значение. Оценка рисков должна сопровождаться оценкой уязвимостей. На этом этапе организация должна растравить приоритеты одних уязвимостей над другими и выделить ресурсы для их устранения. Оценка рисков также должна состоять из шести этапов:

- область действия;
- сбор данных;
- анализ политик и процедур;
- анализ уязвимостей;

- анализ угроз;
- анализ приемлемых угроз.

Четвертым этапом является оценка уязвимостей. Она тесно связана с оценкой риска на предыдущем этапе. Оценка уязвимостей включает в себя выявление уязвимых ресурсов. Эта фаза проводится с помощью ряда согласованных попыток взлома и тестов на проникновение. Цель состоит в том, чтобы смоделировать реальный сценарий взлома с использованием тех же инструментов и методов, которые может использовать потенциальный злоумышленник. Требуется получить исчерпывающий отчет обо всех уязвимостях, которые есть. На на данном этапе существует несколько проблем. Без соответствующей инвентаризации активов нельзя будет определить, на каких устройствах следует сосредоточиться. Также можно забыть оценить защищенность отдельных хостов, а они тем не менее могут оказаться ключевыми целями для потенциальной атаки. Другая проблема связана с используемыми сканерами уязвимостей. Некоторые сканеры могут предоставлять неверные отчеты об оценке уязвимостей. Но ложные срабатывая в сканерах будут всегда. Важно чательно анализировать отчет, иначе это может привести к растрате ресурсов в организации, когда дело доходит до мер по исправлению уязвимостей.

После оценки уязвимостей следующим этапом является стадия отчетов и исправлений. Этот этап имеет две одинаково важные задачи: отчеты и исправление ошибок. Отчеты помогают системным администраторам понять текущее состояние безопасности в организации и области, где она все еще уязвима. Отчеты обычно создается до момента исправления уязвимостей, чтобы вся информация, собранная на этапе управления уязвимостями, могла беспрепятственно перетекать в этот этап. Исправление запускает реальный процесс завершения цикла управления уязвимостями. Этап управления уязвимостями преждевременно заканчивается после анализа угроз и уязвимостей, а также определения приемлемых рисков. Исправление дополняет это, предлагая решения для противодействия выявленным угрозам и уязвимостям. Все уязвимые ресурсы отслеживаются, после чего принимаются необходимые меры для устранения уязвимостей, а также защиты от последующих эксплойтов. Это самая важная задача в стратегии управления уязвимостями, и если она выполнена надлежащим образом, управление уязвимостями считается успешным. Но на данном этапе также встречается множество проблем, поскольку именно здесь определяются решения для всех уязвимостей. Первая проблема возникает, когда отчеты не покрывают все необходимые сферы и не содержат нужной информации о рисках, с которыми сталкивается организация. Плохо написанный отчет может привести к слабым мерам по исправлению и оставить организацию по прежнему уязвимой к угрозам. Также, процесс исправления может быть поставлен под угрозу из-за отсутствия сотрудничества конечных пользователей. Исправление может привести к простоям, а это то, что пользователям абсолютно не нужно.

Планирование реагирования можно рассматривать как самый простой, но тем не менее очень важный этап в стратегии управления уязвимостями. Он не предоставляет проблем, потому что вся важная работа была проделана на предыдущих этапах. Это важно потому что без него организация по прежнему будет подвержена угрозам. На этом этапе важна только скорость исполнения. Крупные организации сталкиваются с серьезными препятствиями при выполнении из-за большого количества устройств, которые требуют исправлений и обновлений. После выпуска исправлений хакеры быстро пытаются найти способы скомпрометировать организации, в которых их не устанавливали. Это показывает, насколько важна скорость, когда речь идет о планировании реагирования. Исправления должны устанавливаться в тот момент, когда они станут доступны [1]. При планировании реагирования организация должна предложить средства исправления или обновления систем, которые были определены как имеющие определенные риски или уязвимости. Следует придерживаться иерархии серьезности угроз, определенной на этапах оценки риска и уязвимостей. Этот шаг должен быть реализован с помощью инвентаризации активов, чтобы организация могла подтвердить, что были задействованы все ее ресурсы, как аппаратные, так и программные. Этап планирования реагирования должен быть завершен с учетом того, когда системы мониторинга отправляют оповещения тем, кто реагирует на инциденты.

Таким образом, организации оказываются под давлением необходимости быстро реагировать на динамично растущее число угроз в области кибербезопасности. Поскольку злоумышленники использовали жизненный цикл атаки, организации также были вынуждены разработать жизненный цикл управления уязвимостями. Он предназначен для противодействия усилиям злоумышленников самым быстрым и эффективным методом.

Список использованных источников:

1. Диогенес Ю, Озкайя Э. Кибербезопасность: стратегии атак и обороны. – М. : Изд-во ДМК, 2020 . – 323 с.

2. Rawan K.. Today’s Inventory Management Systems: A Tool in Achieving Best Practices in INdian Business // Anusandhanika, 2015. №7 – P. 128-135.

ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕВАРИТЕЛЬНОМ ЭТАПЕ ПРОВЕДЕНИЯ АТАКИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мажейко А.М.

Белоусова Е.С. – канд. техн. наук

В работе представлена актуальность этапа предпосылки проведения атаки на информационную систему и роль пользователя, как наиболее уязвимого компонента системы защиты. Установлено, что для решения данной проблемы необходимо использовать дополнительные автоматизированные или административные блоки принятия решений.

Как известно, хакерская атака представляет собой набор определенных последовательных действий для достижения определенной цели. Порядок базовых этапов приведен на рисунке 1.

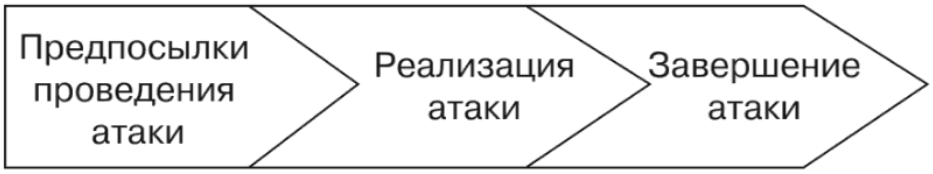


Рисунок 1 – Этапы проведения хакерской атаки [1]

Начиная от исследования и зондирования атакуемой системы, получения к ней доступа и набора необходимых прав и до реализации непосредственной атаки с последующим «заметанием» следов. Существующие системы защиты информации позволяют ставить ограничительные барьеры для действий на каждом из этапов. Однако подавляющее большинство используемых средств защиты направлено на предотвращение атак на этапе «Предпосылки проведения атаки».

Существование термина «человеческий фактор» ставит под угрозу большинство систем защиты. Приведем несколько примеров:

– непреднамеренная загрузка вредоносного программного обеспечения легитимным пользователем на компьютер и последующее неправомерное пользование ресурсами корпоративной сети злоумышленником;

– компрометация ключа доступа к системе (логина, пароля и др.);

– умышленное предоставление доступа нелегитимному лицу легитимным пользователем и последующая эксплуатация уязвимости («исправить ошибку на компьютере», «установить приложение» и прочее).

В приведенных примерах есть общая уязвимая точка – пользователь. Тем или иным способом он является добровольным проводником хакера для получения доступа к системе. Уязвимость состоит в том, что первичные этапы защиты – межсетевые экраны, парольная защита, системы обнаружения вторжений (IDS) – в данном случае оказываются бессильными и пропускают угрозу, т.к. по сути воздействие распознается как действие зарегистрированного пользователя. Пострадавшая организация в данном случае может обнаружить проблему далеко не сразу, даже при наличии в ее штате работников по защите информации и последующем анализе деятельности пользователей. Таким образом для решения проблемы требуются дополнительные технические средства, направленные на выявление необычной деятельности пользователей, и добавление дополнительного блока принятия решений (автоматизированным или административным). В случае автоматизированного решения допускается «жесткий» и «мягкий» подход. Под «жестким» понимается блокировка доступа пользователя к ресурсу до момента снятия блока администратором. В «мягком» подходе используется запрос дополнительных аутентификационных данных пользователя, которые не используются в базовом режиме работы.

Учитывая вышеперечисленную проблему можно утверждать, что разработка и совершенствование средств анализа поведения пользователей в информационной среде является перспективным продолжением развития технологий защиты информации. Здесь можно наблюдать несколько преимуществ. В первую очередь данное направление позволяет автоматизировать процесс реагирования на нетипичное поведение пользователей, а также внутренних нарушителей. Во-вторых, информирование администратора сети или администратора защиты информации становится своевременным и приводит к более быстрому и точному устранению угрозы.

Список использованных источников:
1. Шаньгин, В.Ф. Защита компьютерной информации / В.Ф. Шаньгин. – М. : ДМК Пресс, 2010. – 544 с.

МЕТОДИКА ОЦЕНКИ УРОВНЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА С ПОМОЩЬЮ SDR ПРИЕМНИКА

Белорусский государственный университет информатики и радиоэлектроники, Минск, Республика Беларусь

Маласай В. А.

Борботько Т. В. - доктор техн. наук, профессор

В настоящее время известно достаточное количество сценариев похищения данных с персонального компьютера. Канал утечки информации за счет побочных электромагнитных излучений (ПЭМИ) является далеко не новым. Однако в силу особенностей, связанных со значительной дальностью перехвата, возможностью бесконтактного съёма информации, а также из-за развития и доступности технических средств разведки, он остаётся достаточно опасным.

Средства вычислительной техники (СВТ), обрабатывающие защищаемую информацию, можно рассматривать как совокупность элементарных электрических и магнитных излучателей. При обработке, хранении и передаче информации СВТ возникает изменение электрических токов, проходящих по токопроводящим элементам и образование разности потенциалов между различными точками цепи, которые в свою очередь порождают электрические и магнитные поля.

Узлы и элементы СВТ, в которых возникают большие перепады напряжения и достаточно малые токи, формируют в ближней зоне электромагнитное поле с преобладанием электрической составляющей. Узлы и элементы СВТ, в которых протекают большие токи, и возникают относительно малые перепады напряжения, создают в ближней зоне электромагнитное поле с преобладанием магнитной составляющей. Именно поэтому при измерении ПЭМИ важно рассматривать обе составляющие электромагнитного поля.

Восстановление информации при перехвате излучений цепей, по которым передается видеосигнал, — это один из тех случаев, когда при использовании многоразрядного (как минимум три разряда для цветного монитора) параллельного кода формат представления информации позволяет восстанавливать большую ее часть (теряется цвет, но может быть восстановлено смысловое содержание), не восстанавливая при этом последовательности значений каждого разряда кода.

К безопасным информативным излучениям ПК можно отнести из лучения цепей, формирующих шину данных системной шины и внутреннюю шину данных микропроцессора, а также излучения других цепей, служащих для передач информации, представленной в виде многоразрядного параллельного кода.

С помощью resistor-transistor logic Software defined radio (RTL-SDR) приёмников (программно-определяемое радио) можно принимать сигналы, декодировать их, а также раскладывать на составляющие. Одной из задач исследования является определение эффективности применения приёмника на практике для определения наличия ПЭМИ технических средств в качестве недорогого аналога сертифицированных комплексов. В настоящее время на рынке существует достаточное количество SDR донглов. Все их можно разделить на два типа: 1. Устройства, позволяющие работать только в качестве приёмной стороны; 2. Устройства, позволяющие работать в качестве как приёмника, так и передатчика (полудуплексный метод).

Экспериментально с помощью RTL-SDR приемника исследованы источники побочных электромагнитных излучений монитора (VGA/DVI интерфейсы). Таким образом, проведены экспериментальные исследования утечек информации за счет ПЭМИ по интерфейсам VGA, DVI монитора, и выполнен сравнительный анализ результатов с результатами, полученными с помощью профессионального измерительного комплекса. По каждому из рассмотренных интерфейсов представлены амплитудно-частотные характеристики [6]. Максимальная разница опасных сигналов по частоте у сравниваемых комплексов не превышает 6 кГц, что свидетельствует о возможности применения RTL SDR приемника в учебных целях. Разницу частот можно объяснить несовершенством самого RTL-SDR приемника и большим количеством внутренних шумов на высоких частотах. По результатам исследований разработан лабораторный стенд по обнаружению ПЭМИ, с помощью которого обучающиеся знакомятся с физическими принципами обнаружения утечек информации за счет ПЭМИ.

Оценка защищённости информации на объекте вычислительной техники (ОВТ) по каналу ПЭМИ является обязательной частью при аттестации соответствующего объекта информатизации.

Список использованных источников:

Алексеенко В.И., Петраков А.В., Лагутин В.С. Техническая защита информации / Алексеенко В.И., Петраков А.В., Лагутин В.С. // Вестник связи – 1994. [Электронный ресурс]. - Режим доступа: https://www.twirpx.com/file/26236/ - Дата доступа: 14.12.2019.

Лысов А.В., Остапенко А.Н. Промышленные шпионаж в России: методы и средства / Лысов А.В., Остапенко А.Н. // СПб.: Лаборатория ППШ – 1994. [Электронный ресурс]. - Режим доступа: http://www.bnti.ru/showart.asp?aid=729&lvl=04. - Дата доступа: 21.12.2019.

Максимов Ю.Н., Сонников В.Г., Петров В.Г. Технические методы и средства защиты информации / Максимов Ю.Н., Сонников В.Г., Петров В.Г. // СПб.: ООО «Издательство Полигон» – 2000. [Электронный ресурс]. - Режим доступа: https://search.rsl.ru/ru/record/01000687101 - Дата доступа: 05.01.2020.

Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации / Хорев А.А. // М.: НПЦ «Аналитика» – 2008. [Электронный ресурс]. - Режим доступа: https://booksee.org/book/597367 - Дата доступа: 14.02.2020.

ДЕТЕКТИРОВАНИЕ СЕТЕВЫХ АТАК С ИСПОЛЬЗОВАНИЕМ УСТРОЙСТВ МОНИТОРИНГА И КОНТРОЛЯ ТРАНЗИТНОГО ТРАФИКА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мурашко Е. А., Марычев Д.В.

Петров С.Н. – к.т.н., доцент

В настоящее время отсутствует общий подход к решению проблемы обнаружения аномальных ситуаций во время обработки информации компьютерными системами и информационными сетями. Однако в условиях активного развития информационных технологий и постоянной модернизации программного и аппаратного обеспечения компьютерных систем, решение задач обнаружения аномалий не может обеспечивать безопасность системы. Методы обнаружения аномалий часто применяются для решения задач обнаружения атак на вычислительные системы и информационные сети. Они выбираются применительно к определенному набору параметров системы, и их эффективность зависит только для этого набора параметров.

Детектирование атак с использованием программно-аппаратных средств защиты информации способствуют своевременному обнаружению проблем, которые могут привести к успешным противозаконным действиям со стороны злоумышленника. Другими словами, обнаружение уязвимости на этапе тестирования позволяет разработчикам технических и программных продуктов заблокировать все возможные варианты незаконных действий злоумышленника для получения выгоды.

Методика детектирования атак позволяет определить, какое максимальное количество атак может обнаружить и предотвратить устройство без потери данных, что позволяет распределить все категории программно-аппаратных продуктов на определенные сценарии их использования, а также их пригодность для использования в сетях различных организаций. Результаты тестирования помогают увидеть, какими функциональными возможностями может обладать устройство, либо программный продукт, что позволит потенциальному покупателю, увидев заключения экспертов, определить, какое именное решение правильнее и выгоднее всего использовать в организации сетевой инфраструктуры компании либо предприятия.

Современные методы детектирования атак с использованием программно-аппаратных средств защиты информации имеют широкое распространение в жизни сообщества информационных технологий, но подразумевает собой засекречивание методик испытаний. Данный факт имеет место по причине того, что в ситуации, когда методика испытаний продукта находится в общем доступе, потенциальный злоумышленник может видеть места, через которые легче всего если не полностью перехватить информацию, то нанести ей вред.

Для проведения тестирования программно-аппаратных средств защиты информации необходимо соответствующее оборудование, средства соединения через каналы связи, соответствующие определенным требованиям и специализированное программное обеспечение.

Существует несколько основных типов реализации системы тестирования: система на основе аппаратного тестового стенда, система на основе виртуальной сетевой инфраструктуры, а также смешанный тип. Каждый из приведенных типов имеет преимущества при тестировании той или иной категории программных и программно-аппаратных средств защиты информации. Также определенные средства защиты информации возможно протестировать только лишь на определенном типе тестового стенда. Для проведения испытаний на ПЭВМ испытательного стенда устанавливается следующее ПО:

Таблица 1 – Перечень программного обеспечения

№п/п	ПЭВМ (ВМ)	Перечень программного обеспечения
1	ПЭВМ 1	ОС Microsoft Windows 7 Professional; утилита Wireshark версия 2.0.7; утилита Iperf; почтовый клиент Thunderbird версии 52.4.0; утилита Small HTTP Server 3.05.93;
2	ПЭВМ 2	ОС Kali Linux 2.0;
3	ПЭВМ 3	ОС Windows Server 2013; утилита Iperf; Small HTTP Server 3.05.93; VMware Workstation 12 Версия 12.5.2:

№п/п	ПЭВМ (ВМ)	Перечень программного обеспечения
4	ВМ 1	ОС Microsoft Windows 7; Courier Mail Server; RADIUS сервер.
5	ВМ 2	ОС Ubuntu 8.04; Web-приложение bWAPP v2.2 (приложение уязвимое к SQL инъекциям и межсайтовому выполнению сценариев XSS).

Персональные электронные вычислительные машины, коммутаторы и тестируемое программно-аппаратное СЗИ соединяются кабелями UTP категории 6 в соответствии со схемой, указанной на рисунке 1. При наличии разъемов для SFP/SFP+ модулей используются волоконно-оптические кабели.

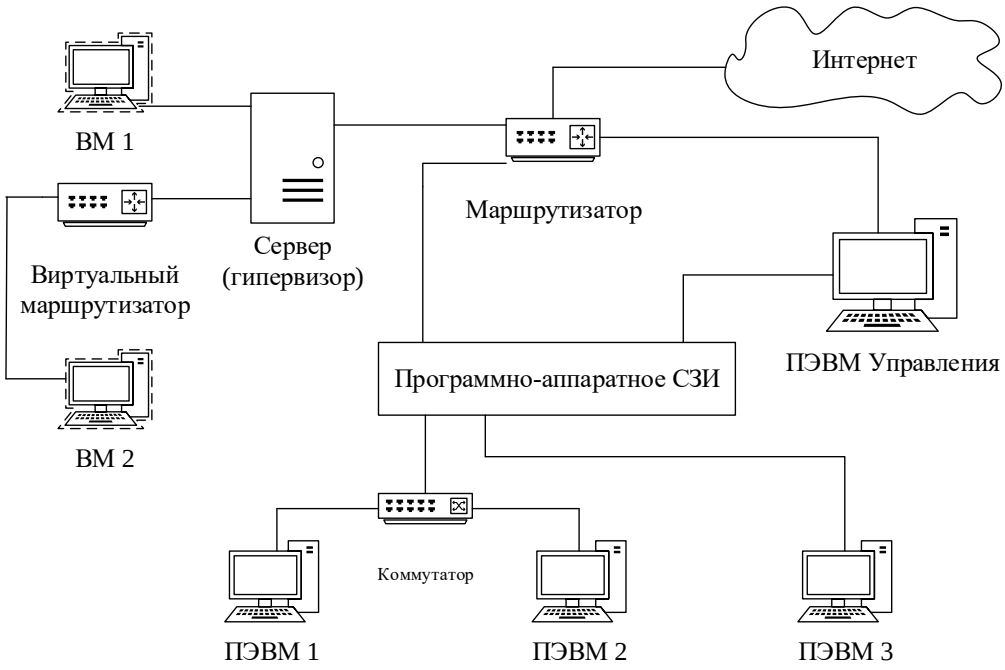


Рисунок 1 – Схема испытательного стенда

Рассмотренная система несет в себе цель оценки соответствия, поиска недостатков программно-аппаратных СЗИ, что необходимо для усовершенствования разработок производителей в области защиты информации. Получение подробных данных о продукте и об обрабатываемым им атаках помогает потенциальному покупателю системы быть уверенным в безопасности данного устройства, а также в безопасности передачи данных, которое данное устройство обеспечивает. Соответственно тестирование согласно методике испытаний является неотъемлемой частью разработки функционального продукта, а результат тестирования на обнаружение сетевых атак – гарантом реализации трех основных постулатов информационной безопасности: конфиденциальности, целостности и доступности данных

Список использованных источников:

1 Компьютерные системы и сети [Электронный ресурс]. – Режим доступа : http://www.kcc.ru.

2 В.Г. Олифер, Н.А. Олифер. Компьютерные сети, принципы, технологии, протоколы (2-е издание) [Электронный ресурс]. – Режим доступа: https://www.bsuir.by/m/12_100229_1_85460.pdf.

3 Архитектура локальных сетей типа Ethernet [Электронный ресурс]. – Режим доступа http://sgpek.ru/files/electronbook/ISS/l9.html.

4 IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific [Электронный ресурс]. – Режим доступа : http://standards.ieee.org.

5 Ю.А. Родичев. Нормативная база и стандарты в области информационной безопасности [Учебное пособие]. – Режим доступа: https://search.rsl.ru/ru/record/01008599511.

6 Полторак А.А. Методы обнаружения сетевых аномалий в облачных средах [Электронный ресурс]. – Режим доступа: https://sibac.info/archive/meghdis/11(46).pdf (дата обращения: 01.07.2019)

7 С.Ю. Микова, В.С. Оладько, М.А. Нестеренко. Подход к классификации аномалий сетевого трафика [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/podhod-k-klassifikatsii-anomaliy-setevogo-trafika

8 Е.В. Ананьгин, И.С. Кожевникова, А.В. Лысенко, А.В. Никишова. Методы обнаружения аномалий и вторжений. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/metody-obnaruzheniya-anomaliy-i-vtorzheniy

9 А. А. Браницкий, И. В. Котенко, Анализ и классификация методов обнаружения сетевых атак, Тр. СПИИРАН, 2016, выпуск 45, 207–244 [Электронный ресурс]. – Режим доступа: http://www.mathnet.ru/links/1caa527ffecf29541261d48d0c84db5c/trspy873.pdf

ЗАЩИТА ЦИФРОВЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ ОТ ПОМЕХ

Певзнер В.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ильинков В.А. – канд. техн. наук

Исследованы различные методы моделирования цифровых сигналов различных форматов и квазиоптимальных сигналов. Произведено моделирование процесса прохождения сигналов через каналы связи, представленные в виде некоторого количества фильтров нижних частот.

Системы инфокоммуникаций (СИК), являющиеся неотъемлемой составной частью современного информационного общества, характеризуются следующей совокупностью существенных признаков [1]:

– наиболее динамично развивающаяся область науки и техники, следствием чего является быстрое увеличение объёма информации и малое время жизни производимых моделей;

– многообразие систем и устройств различного функционального назначения, высокие требования к их параметрам качества;

– необходимость обеспечения целостности и доступности передаваемых данных;

– и др.

Учитывая изложенное, основным инструментом исследования, проектирования и разработки современных СИК принято считать моделирование [2]

Моделирование на основе операционного исчисления получило большое распространение при анализе и синтезе систем.

В качестве воздействия при моделировании линейных искажений целесообразно использовать сигналы, представляемые совокупностью одной или нескольких элементарных кривых (отрезков прямых, гармонических функций и т.д.). Лапласовское изображение указанного воздействия, получаемое на основании прямого преобразования Лапласа, является мероморфной функцией комплексного переменного (однозначная функция называется мероморфной, если ее особенностями являются только полюсы), причем, не сужая круга применимости модели, можно всегда выбрать такой вид, чтобы изображение содержало только однократные полюсы, не совпадающие с полюсами операторной передаточной функции моделируемого звена (канала) [3]. Зная изображение и передаточную функцию, находим вначале изображение реакции, а затем, применяя обратное преобразование Лапласа, – саму реакцию (выходной сигнал)

Общий алгоритм проведения исследования может быть следующим:

1. Анализ и оценка существующих методов моделирования сигналов и звеньев с последующим обоснованием сделанного выбора;
2. Математические моделирование сигналов, каналов связи и реакций каналов на воздействия.
3. Оценка полученных результатов с целью оптимизации параметров системы для обеспечения большей помехозащищенности.
4. Разработка прикладного программного обеспечения для автоматизации изложенных выше задач.

Список использованных источников:

1. Локшин Б. А. Цифровое вещание: от студии к телезрителю/ Б. А. Локшин – М.: Радио и связь, 2001. – 354 с.
2. Борисов, Ю. П. Математическое моделирование радиотехнических систем и устройств / Ю. П. Борисов, В. В. Цветнов. – М. : Радио и связь, 1985. – 176 с.
3. Лаврентьев, М. А. Методы теории функций комплексного переменного: учебник для вузов / М. А. Лаврентьев, Б. В. Шабат ; изд. 6-е, стереотип. – СПб. : Лань, 2002. – 688 с.

ЗАЩИТА ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ ОТ ИНФОРМАЦИОННЫХ АТАК

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Полещук В.С.

Ширинский В.П. – к.т.н.,доцент

Изложены причины возникновения информационных атак, их сущность и стадии развития (жизненный цикл). Дается обзор средств обнаружения и предотвращения атак, принципы действия данных систем и перспективы развития.

Уровень криминогенности в информационной сфере сетей передачи данных ведущих стран мира постоянно повышается, несмотря на интенсивное внедрение вновь создаваемых технологических решений в области информационной безопасности. Это приводит к миллиардным финансовым потерям в глобальном масштабе. Проблема усугубляется также постоянным ростом уровня сложности информационных атак.

В свете вышеизложенного, защита ИКС от информационных атак является одной из наиболее актуальных и значимых задач в области индустрии интернет-технологий (ИТ-индустрии).

Практически любая автоматизированная система может выступать в качестве объекта информационной атаки, которая может быть определена как совокупность действий злоумышленника, направленная на нарушение одного из трех свойств информации — конфиденциальности, целостности или доступности.

Основной причиной возникновения информационных атак являются уязвимости. Наличие самих слабых мест в ИКС может быть обусловлено самыми различными факторами, начиная с простой халатности сотрудников и заканчивая преднамеренными действиями злоумышленников.

Уязвимости могут присутствовать как в программно-аппаратном, так и в организационно-правовом обеспечении ИКС.

Уязвимости программно-аппаратного обеспечения могут присутствовать в программных или аппаратных компонентах рабочих станций пользователей ИКС, серверов, а также коммуникационного оборудования и каналов связи ИКС. В соответствии с трехуровневой моделью узла ИКС, уязвимость может быть отнесена к аппаратному обеспечению, а также к общесистемному или прикладному ПО. В том случае, если уязвимость содержится в программно-аппаратном обеспечении ИКС, которое отвечает за организацию сетевого взаимодействия между узлами ИКС, она может быть дополнительно соотнесена с одним из пяти уровней модели BOC - физическим, канальным, сетевым, транспортным или прикладным.

В отдельных случаях ошибки и недостатки могут содержаться не только в программно-аппаратном обеспечении ИКС, но и в спецификациях и стандартах, описывающих протоколы стека TCP/IP. В основном такие недостатки связаны с отсутствием в протоколах встроенных средств защиты, что делает их уязвимыми к различным информационным атакам.

Любая атака в общем случае может быть разделена на четыре стадии:

-Стадия рекогносцировки. На этом этапе нарушитель осуществляет сбор данных об объекте атаки, на основе которых планируются дальнейшие стадии атаки.Собираемая информации может включать тип и версию операционной системы (ОС), установленной на узлах ИКС, список пользователей, зарегистрированных в системе, сведения об используемом прикладном ПО и др

-Стадия вторжения в ИКС. На этом этапе нарушитель получает несанкционированный доступ к ресурсам тех узлов ИКС, по отношению к которым совершается атака.

-Стадия атакующего воздействия на ИКС. Данный этап направлен на достижение нарушителем тех целей, ради которых предпринималась атака. Примерами таких действий могут являться нарушение работоспособности ИКС, кража конфиденциальной информации, хранимой в системе, удаление или модификация данных системы и др. При этом атакующий может также осуществлять действия, которые могут быть направлены на удаление следов его присутствия в ИКС.

Стадия дальнейшего развития атаки. На этом этапе выполняются действия, которые направлены на продолжение атаки на ресурсы других узлов ИКС.

Изначально для обнаружения и отражения сетевых атак использовались межсетевые экраны (для блокирования сетевых соединений в процессе атаки) и разнообразное антивирусное ПО, срабатывающее, как правило, на 2-й и 3-ей стадиях. Однако данные средства показали свою ограниченную эффективность, что привело к появлению отдельных систем для обнаружения и отражения сетевых атак - IDS (intrusion detection system) и IPS (intrusion prevention system).

Задача IDS состоит в обнаружении и регистрации атак, а также оповещении при срабатывании определенного правила. В зависимости от типа, IDS умеют выявлять различные виды сетевых атак, обнаруживать попытки неавторизованного доступа или повышения привилегий, появление вредоносного ПО, отслеживать открытие нового порта и т. д. Однако, в отличие от межсетевого экрана, контролирующего только параметры сессии (IP, номер порта и состояние связей), IDS «заглядывает» внутрь пакета (до седьмого уровня OSI), анализируя передаваемые данные. Существует несколько видов систем обнаружения вторжений. Весьма популярны APIDS (Application protocol-based IDS), которые мониторят ограниченный список прикладных протоколов на предмет специфических атак. Типичными представителями этого класса являются PHPIDS, анализирующий запросы к PHP-приложениям, Mod_Security, защищающий веб-сервер (Apache), и GreenSQL-FW, блокирующий опасные SQL-команды.

Сетевые NIDS (Network Intrusion Detection System) более универсальны, что достигается благодаря технологии DPI (Deep Packet Inspection, глубокое инспектирование пакета). Они контролируют не одно конкретное приложение, а весь проходящий трафик, начиная с канального уровня.

Системы IDS предназначены только для сигнализации обо всех все подозрительных действиях. Чтобы заблокировать атакующий хост, системный администратор самостоятельно перенастраивает брандмауэр во время просмотра статистики. В таком случае, однако, о реагировании в реальном времени речи не идет. Именно поэтому в настоящее время появились IPS (Intrusion Prevention System, система предотвращения атак). Они основаны на IDS, но могут самостоятельно перестраивать пакетный фильтр или прерывать сеанс, (например, отсылая TCP сообщение RST по протоколу TCP). В зависимости от принципа работы, IPS может устанавливаться «в разрыв» или использовать зеркалирование трафика (SPAN), получаемого с нескольких сенсоров. Примерами таких систем являются IBM Security Network Intrusion Prevention System, McAfee Network Security Platform, Suricata и др.

Однако современный Интернет несет огромное количество угроз, поэтому узкоспециализированные системы уже не актуальны. В связи с этим необходимо использовать комплексное многофункциональное решение, включающее все компоненты защиты: файервол, IDS/IPS, антивирус, прокси-сервер, контентный фильтр и антиспам-фильтр. Такие устройства получили название UTM (Unified Threat Management, объединенный контроль угроз). В качестве примеров UTM можно привести Trend Micro Deep Security, Kerio Control и др.

Список использованных источников:
В. Сердюк. Новое в защите от взлома корпоративных сетей // Техносфера. М. 2007 С.11–63.

МАГНИТНЫЕ ХАРАКТЕРИСТИКИ НАНОЧАСТИЦ КОБАЛЬТА НА ПОДЛОЖКЕ ИЗ КРЕМНИЯ И ВНУТРИ УНТ

Прокопюк Е.Н.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Прищепа С.Л. – проф., д.ф.- м.н.

Работа содержит исследование магнитных свойств плотноупакованных наночастиц кобальта.

Исследовались магнитные свойства ансамбля плотноупакованных наночастиц Co осажденных на подложки из кремния. Плотность расположения наночастиц составляла $1{,}2\times10^{10}$ см$^{-2}$, средний размер наночастиц был 15 ± 5 нм. На рисунке 1а показано изображение, полученной на магнитном силовом микроскопе (МСМ) тестового образца, который представлял из себя наночастицы Co на подложках SiO_2/Si, а на рисунке 1б – для Co-УНТ образца.

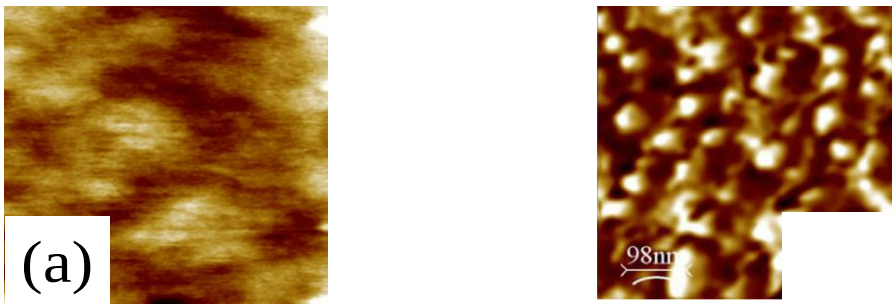


Рисунок 1 – МСМ изображение для наночастиц Co на подложке Si/SiO_2 (а) и Co-УНТ (б)

В первом случае магнитные домены представляют собой области размером порядка 500 нм, что включает порядка сотни наночастиц. Это однозначно свидетельствует о сильном дипольном взаимодействии между ними. Для образца Co-УНТ, выращенного из тестового, средний размер магнитного диполя составляет порядка 50 нм, что близко к размеру наночастицы кобальта на вершине нанотрубок. Больший размер диполя по сравнению с физическим размером наночастиц вызван удаленностью иглы магнитного силового микроскопа от поверхности образца. Данный результат свидетельствует о магнитной изолированности наночастиц кобальта внутри УНТ друг от друга.

Магнитоизоляция наночастиц Co внутри УНТ обусловлена дополнительными механическими напряжениями, возникающими в кобальте при использовании его в качестве катализатора при росте УНТ методом химического парофазного осаждения. Эти напряжения усиливают магнитоупругую анизотропию, что приводит к преодолению дипольного взаимодействия между плотноупакованными наночастицами Co.

ОСОБЕННОСТИ РАЗРАБОТКИ МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ЗАЩИЩЁННОГО ОБМЕНА СООБЩЕНИЯМИ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ С ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ BLOCKCHAIN

Романовский М.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. тех. наук

Аннотация. Одним из способов реализации приложения с безопасным обменом сообщений является использование blockchain технологии, обеспечивающей следующие возможности: криптографическая защита сообщений; создание аккаунта используя faucet; авторизацию echo аккаунта; создание комнаты для чата; подключение к уже созданной комнате; QR-code для простоты подключения к созданной комнате; получение и отправка сообщений в рамках комнаты.

Для описания логики работы передачи данных необходимо рассмотреть термин smart контракт, заключающийся в описании сущности процесса, к которому стремиться разработчик, использующий технологию blockchain.

В настоящее время существуют различные фреймворки облегчающие внедрение технологии blockchain. Рассмотрим вариант использования фреймворка echo-androidframework, находящегося в свободном доступе. Для его применения в приложении должны быть дополнительно реализованы следующие компоненты: подключение фреймворка в проект и инициализация клиента.

Важной частью разработки мобильного приложения является написание smart контракта, который разрабатывается на языке solidity и выглядят, чаще всего, как стандартный объектно-ориентированный класс. Поля и блок конструктора smart контракта для обмена сообщениями в режиме реального времени выглядит следующий образом:

```
public contract ChatRoom {
  struct Messages {
            string ownerMessages;
            string companionMessages;
  }
  address owner;
  address companion;
  mapping(uint256 => Messages) messages;
  constructor(address companionAddress) public
  {
            owner = msg.sender;
            companion = companionAddress;
  }
}
```

Для работы приложения должны быть реализованы следующие функции smart контракта.

1. Отправка сообщений посредством function uploadMessage(string message).
2. Получение сообщений собеседника на основе использования function getCompanionMessages(uint256 blockNum) public view returns (string savedMessages).
3. Проверка наличий сообщений собеседника с помощью function haveCompanionMessages(uint256 blockNum) public view returns (bool value).
4. Проверка разрешения на присоединение к комнате, используя function canJoinRoom() public view returns (bool value).

Таким образом, использование технологии blockchain и фреймворка echo-android совершенствует приложение, упрощает процесс разработки и уменьшает количество используемых ресурсов. Необходимо отметить, что данная технология имеет преимущества децентрализации, открытости и надёжности с высоким уровнем криптографической защиты.

Список использованных источников:

1. Баулин А. Блокчейн в эфире // Форбс / Forbes. – 2017. – № 11.– С. 126–127.
2. Вахранев А. В. Роль биткоинов в экономике и их производство // Бизнес в законе. – 2016. – № 6. – С. 224–226
3. Генкин А. С. Блокчейн и уникальные ценные объекты // Страховое дело. – 2017. – № 3. – С. 15–22.

СИСТЕМЫ МОНИТОРИНГА СЕТЕВОГО ОБОРУДОВАНИЯ СЕТИ WI-FI

Савичев А.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Цветков В.Ю. – доктор технических наук

В работе приведён сравнительный анализ существующих и свободно распространяемых систем мониторинга оборудования сети Wi-Fi. Сделаны выводы о явных преимуществах и недостатках сравниваемых систем.

1.Microsoft SCOM – System Center Operations Manager – система сквозного мониторинга от Microsoft, в том числе активного слежения за состоянием сетей (наблюдение за любыми сетевыми устройствами, поддерживающими SNMP, вплоть до уровня портов, а также обнаружение виртуальных локальных сетей и коммутаторов в таких сетях).

Основные достоинства:

– исключительная производительность и работоспособность приложений для программных сред Microsoft;

– обеспечивает сквозное управление службами для сервисов вашего центра обработки данных;

– способствует улучшению эффективности и управления средами центров обработки данных;

– унифицированный контроль в рамках частных и общедоступных облачных сервисов;

– поддержка Windows PowerShell 2.0 с набором новых командлетов;

Одно из главных достоинств System Center Operations Manager – продвинутая визуализация всего огромного собранного набора данных, в основном в виде графиков и диаграмм, причём визуализация доступна не только в специальной консоли программы, но и через веб-интерфейс.

Основные недостатки:

– система мониторинга охватывает множество общих показателей системы, но непригодна для слежения за специфическими параметрами;

– до сих пор работа с операционными системами вне семейства Windows нестабильна;

– необходимость установки сервиса агента;

– невероятная громоздкость и трудоёмкость настройки продукта «под себя»: система дольше подходит для мониторинга общего состояния и сбора основных сведений о большой структуре (например, множество клиентских и серверных машин в домене).

Также существенный недостаток системы состоит в высокой стоимости данного программного продукта.

2.Zabbix – свободно распространяемая система для комплексного мониторинга сетевого оборудования, серверов и сервисов.

Основные достоинства:

– вся конфигурация хранится в базе и управляется через веб-интерфейс;

– единая точка доступа для пользователей;

– разграничения доступа к данным и конфигурации;

– встроенные богатые средства визуализации;

– развитые возможности анализа собранных данных;

– предоставляет гибкие возможности по настройке условий-триггеров, которые включаются при авариях и неполадках;

Основные недостатки:

– все данные истории хранятся в базе, что неэффективно и ограничивает масштабируемость;

– не обеспечивается отказоустойчивость;

– мониторинг серверов и рабочих станций осуществляется через постоянно запущенный агент;

В качестве дополнительного минуса стоит отметить сложность делегирования прав – машина с сервисом зачастую управляется операционной системой семейства *nix, что делает трудоёмким взаимодействие с доменными пользователями и правами из Active Directory (Windows системы).

3.Nagios – (первоначально Netsaint) – свободно распространяемая программа для мониторинга систем и сетей.

Основные достоинства:

– простой формат конфигурационного файла. При наличии минимального опыта в программировании можно написать собственные плагины для Nagios;

– позволяет оставлять комментарии с меткой времени;

– существуют плагины на все случаи жизни от сторонних производителей;

– отправка оповещений в случае возникновения проблем со службой или хостом (с помощью почты, смс, или любым другим способом, определенным пользователем через модуль системы);

Основные недостатки:

– нет возможности конфигурирования через веб-интерфейс. Все изменения конфигурации выполняются правкой файлов конфигурации с последующим полным перезапуском сервера Nagios;

– слишком большой интервал между проверками и замерами параметров;

– отсутствуют встроенные средства визуализации (кроме карты сети);

– сложность масштабирования без использования плагинов от сторонних производителей;

– каждый плагин запускается как отдельный процесс;

Дополнительно к недостаткам можно отнести проблемное взаимодействие с серверами под управлением Windows.

4.Cacti – бесплатное приложение мониторинга, позволяющее собирать статические данные за определённые временные интервалы и отображать их в графическом виде при помощи RRDtool утилиты, предназначенной для работы с круговыми базами данных (Round Robin Database), которые используются для хранения информации об изменении одной или нескольких величин за определенный промежуток времени.

Основные достоинства:

– высокая скорость развертывания при минимальном дополнительном кодировании;

– простота и удобство интерфейса просмотра диаграмм и их настройки;

– возможность подключения скриптов;

Основные недостатки:

– сложен в первоначальной настройке;

– отсутствие возможности инвентаризации;

– ограниченная производительность «неродных» JMX решений для Cacti;

Так же отдельным недостатком можно выделить довольно быстрое нарастание количества однотипных настроек в случае большого числа сред и серверов.

5.Observium – является системой мониторинга и наблюдения за сетевыми устройствами и серверами. При этом список поддерживаемых устройств огромен и не ограничивается только сетевыми устройствами, главное условие — чтобы устройство поддерживало работу SNMP.

Основные достоинства:

– имеет огромнейший список систем, за которыми может производить мониторинг;

– предустановленные шаблоны для SNMP OID;

– отображение графиков, аппаратных ресурсов, датчиков в удобном для пользователя виде;

– подключение Syslog сообщений;

Основные недостатки:

– система оповещений доступна только в платной версии;

– работа с картами местности доступна только через Google карты;

– ограничен 5-ти минутным интервалом опроса устройств;

В результате анализа сравниваемых систем мониторинга выявлены следующие критические минусы:

– нет системы оповещений в Cacti;

– при использовании RRD в Cacti и Nagios теряется детализация старых данных;

– конфигурация в Nagios изменяется посредством изменения файла конфигурации, но новая конфигурация применяется только при перезапуске службы Nagios, что при большом количестве собираемых метрик может занимать несколько десятков минут, а следовательно, система не будет функционировать в это время.

Zabbix имеет менее критические недостатки, связанные с визуализацией данных, что слабо влияет на основные функциональные возможности системы. Наименее ресурсоемкой системой является Cacti и Observium, наиболее ресурсоемкой – Nagios и Zabbix. Но из-за описанных недостатков и необходимости использования большого количества сторонних плагинов для Cacti и Nagios, а также из-за сложности масштабирования этих систем наилучшим выбором для мониторинга большого количества метрик признан Zabbix и Observium.

Список использованных источников:

1. Основы мониторинга и сбора метрик. URL: https:// www.8host.com/blog/osnovy-monitoringa-i-sbora-metrik..
2. Шмелев В. В. Метод мониторинга технологических процессов на основе структурно-логического подхода // Интеллектуальные технологии на транспорте. 2017. № 2. С. 5-14.
3. Линикова О. Е. Мониторинг серверного оборудования и приложений. – Екатеринбург, 2014.

ПРИМЕНЕНИЕ ОБЛЕГЧЁННЫХ КРИПТОАЛГОРИТМОВ ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Анисимова Ю.Н., Савченко А.А.
Власова Г.А. – к.т.н.,доцент

Основные проблемы обеспечения безопасности устройств Интернет вещей обусловлены тем, что существующие методы и средства защиты изначально разрабатывались для персональных компьютеров, и не учитывали особенности и ограничения устройств Интернета вещей. Для защиты таких устройств необходимо применять облегчённые криптографические алгоритмы, эффективность применения которых зависит от специфики устройства и качественного подбора к нему криптоалгоритма.

Интернет вещей (Internet of Things, IoT) – концепция, предполагающая объедение в сеть устройств (вещей), способных взаимодействовать друг с другом на основе встроенных технологий, которые поддерживаются данной сетью. Устройствами (вещами) являются «умные» гаджеты, «умная» техника и другие устройства, которые могут быть использованы в обиходе человека или его дома.

Применение традиционных методов защиты устройств Интернета вещей, таких как шифрование, идентификация/аутентификация и внедрение физических мер обеспечения безопасности, требует их существенного реинжиниринга и адаптации, так как устройства имеют множество ограничений. Интернет вещей, как правило, состоит из портативных устройств с низким электропотреблением, малым форм-фактором и ограниченными возможностями [1].

Основным средством обеспечения информационной безопасности в мире Интернета вещей является так называемая «облегчённая» криптография. К облегчённой криптографии относятся алгоритмы, разрабатываемые специально для устройств с ограниченными или крайне ограниченными вычислительными ресурсами.

Симметричные алгоритмы ввиду своих качеств используются для шифрования видео-данных, где требуются очень производительные системы для шифрования, а также необходима значительная вычислительная мощность для шифрования и декодирования в реальном времени. Стремительное развитие рынка видеонаблюдения показывает, что направлением нового времени является именно IP-видеонаблюдение.

При выборе легковесного криптоалгоритма, реализующего шифрование видео-данных, следует учитывать такие характеристики алгоритма, как длина информационного блока, длина ключа, число раундов (циклов шифрования), влияющие на криптостойкость алгоритма, в данном случае, при шифровании видеоданных, размера ключа в 128 бит и число раундов больше 20 будет достаточно, количество условных логических элементов должно быть в пределе 1000 GE.

Ссылаясь на статью [2], где приведены сравнительные характеристики алгоритмов, и сравнивая по такому параметру, как длина ключа, для обеспечения необходимого уровня криптостойкости подходят алгоритмы LED, Piccolo, PRESENT, TWINE с длиной ключа в 128 бит. Алгоритм LED имеет худшие показатели числа тактов работы, характеристики у Piccolo, PRESENT схожи, однако алгоритм Piccolo имеет преимущество ввиду меньшего количества логических элементов для реализации при таких же показателях длины ключа, числа раундов и числа тактов работы алгоритма.

Ссылаясь на [3], где указаны сравнительные результаты реализации блочных шифров Piccolo-128, TWINE -128, PRESENT-128 на 16-разрядном микропроцессоре RL78 от Renesas Electronics. по параметрам занимаемых ОЗУ, ПЗУ, скорости шифрования и дешифрования, видно, что алгоритмы Piccolo, PRESENT могут быть реализованы с небольшим объемом оперативной памяти, 64 байта оперативной памяти было достаточно во всех категориях. Алгоритм TWINE имеет незначительные программные издержки, что обеспечивает чрезвычайно малый размер кода. С точки зрения скорости, TWINE достиг уровня, аналогичного Piccolo. Для реализации шифрования большого объема данных с IP систем видеонаблюдения с большой скоростью подходит блочный симметричный тип шифрования и реализующий его алгоритм Piccolo-128.

Асимметричная криптография используется в SSL/TLS, которые помогают сделать HTTPS соединение безопасным. К популярным алгоритмам с использованием открытых ключей относятся: RSA, DSA, ECC и PKCS, но все они имеют определенные недостатки, либо сравнительно невысокая скорость работы (напр., алгоритмы на базе эллиптических кривых (ЭК)), либо сравнительно низкая стойкость при сопоставимых

размерах ключей и параметров (схема Диффи-Хеллмана и другие алгоритмы, основанные на дискретном логарифме в поле), либо и то, и другое одновременно (RSA).

В статье [4] приведены сравнения размеров ключей для Number Theorists aRe Us (NTRU) с эквивалентными размерами ключей для систем, основанных на проблемах факторизации целых чисел и дискретного логарифма в группе точек эллиптических кривых. Сравнения показывают, что NTRU имеет все необходимые условия для обеспечения наивысшего уровня стойкости и по этому показателю не отстает от конкурентов.

В [4] приводятся сравнительные результаты измерений скорости NTRU, ЭК и RSA.

NTRU имеет высокую скорость выполнения операций зашифрования/расшифрования. По заявлениям компании Security Innovation, занимающейся разработкой NTRU, данный алгоритм до двухсот раз быстрее, чем алгоритмы на эллиптических кривых и RSA, и при этом его реализация гораздо меньше (около 8 Кб).

Ниже в таблице 1 приводится сравнение алгоритмов NTRU, RSA и ECC-NIST-224. Скорость работы данных алгоритмов была замерена как на ЦПУ, так и на графических процессорах с использованием технологии распараллеливания CUDA от Nvidia. Алгоритмы NTRU, RSA и ECC-NIST-224 представлены в [5].

Таблица 1 – Сравнение скорости реализаций NTRU, RSA и ЭК для ЦПУ и ГПУ

Алгоритм	Языки платформа	Параметры алгоритма	Зашифр/с	Расшифр/с	Бит/опер.
NTRU	Intel Core2 Extreme @ 3.00GHz	(N, q, p) = (1171, 2048, 3) (k = 256)	95	95	1756
	CUDA, GTX280 (1 операция)		571	546	
	CUDA, GTX280		$24*10^3$	$24*10^3$	
RSA	CUDA, Nvidia 8800 GTS	2048 bit (k = 112)	-	104	2048
	Intel Core2 @ 1.83GHz		$6,65*10^3$	168	
ЭК	CUDA, Nvidia 8800 GTS	ECC-NIST-224 (k = 112)	-	$1,41*10^3$	

	Intel Core2 @ 1.83 GHz (ECDSA)			1,86** 10^3	

Можно сделать вывод о высоком уровне стойкости NTRU, который не уступает стойкости алгоритмов на базе эллиптических кривых. Но в связи с новизной и малой распространенностью NTRU необходимо проводить дополнительные исследования на предмет возможных закладок и критических уязвимостей, которые могут быть использованы для разработки эффективных атак. В результате анализа быстродействия NTRU было установлено, что его скорость работы гораздо выше, чем у RSA и ЭК.

Применение облегчённых криптоалгоритмов позволяет обеспечить защиту устройств Интернета вещей с ограниченными вычислительными ресурсами. Микропроцессор на основе асимметричной криптографии могут использоваться в любых гаджетах, где не требуется высокая пропускная способность интернет трафика, например, в гаджетах «умного» дома. Выбор алгоритма для реализации основывается на таких сравнительных характеристиках, как требуемое количество условных логических элементов, занимаемой ОЗУ, ПЗУ, скорости шифрования, скорости дешифрования. Результаты сравнения скорости реализации асимметричных легковесных криптографических алгоритмов показали, что наилучшими параметрами обладает алгоритм NTRU. Результаты сравнения основных параметров реализации симметричных легковесных криптографических алгоритмов показали, что алгоритм Piccolo-128 имеет преимущества и подходит для реализации шифрования большого объема данных с IP-систем видеонаблюдения.

Список использованных источников:

1. Полегенько А. М. Особенности защиты информации в интернете вещей [Текст] / А. М. Полегенько // International Journal of Open Information Technologies. – 2018. - № 6. – С. 41-44.

2 .Жуков А. Е. Легковесная криптография. часть 1 [Текст] / А. Е. Жуков // Вопросы кибербезопасности. – 2015. - № 4. – С. 31-36.

3. Cryptographic Technology Guideline (Lightweight Cryptography) [Текст]: Lightweight Cryptography Working Group / Kazumaro Aoki, Tetsu Iwata, Kazuto Ogawa и др. – Cryptrec, 2017. – С. 39-44.

4. Jens Hermans, Frederik Vercauteren, Bart Preneel. Speed records for NTRU. Department of Electrical Engineering, University of Leuven Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium.

5. Speed records for NTRU [Электронный ресурс]. – Режим доступа: https://homes.esat.kuleuven.be/~fvercaut/papers/ntru_gpu.pdf.

ПРИЛОЖЕНИЕ ДЛЯ СОКРЫТИЯ ИНФОРМАЦИИ В АУДИОФАЙЛЕ МЕТОДОМ ЗАМЕНЫ НАИМЕНЬШЕГО ЗНАЧАЩЕГО БИТА (LSB)

Шахмуть А.М.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Петров С.Н. – к.т.н., доцент

Слово стеганография происходит от греческих слов: «steganos», что дословно означает «скрывать» или «секрет» и «graphy», что означает «письмо» или «рисование». Отсюда, стеганография – это искусство сокрытия секретной информации в файле таким образом, что только отправитель и получатель могут знать о ее наличии. Конфиденциальная информация закодирована так, что само существование сообщения утаивается. Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех странах, в которых запрещена криптография. Таким образом, криптография защищает содержание сообщения, а стеганография защищает сам факт наличия каких-либо скрытых посланий.

Одним из самых распространённых методов является LSB (Least Significant Bit, наименьший значащий бит) алгоритм, который заменяет наименьший значащий бит в нескольких байтах файла-носителя, чтобы скрыть последовательность байтов, содержащих скрытые данные. Это, как правило, эффективно тогда, когда замена младшего бита не влечет за собой значительное ухудшение качества. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека. Небольшая модификация этой стеганографической техники позволяет использовать для встраивания сообщения два или более младших битов на байт. Это увеличивает объем скрытой информации в объекте-контейнере, но скрытность сильно снижается, что облегчает обнаружение стеганографии.

Преимущества метода:

– размер файла-контейнера остается неизменным;

– при замене одного бита в канале синего цвета внедрение невозможно заметить визуально;

– возможность варьировать пропускную способность, изменяя количество заменяемых бит.

Недостатки метода:

– скрытое сообщение легко разрушить, например, при сжатии или отображении;

– не обеспечена секретность встраивания информации, так как точно известно местоположение скрываемой информации.

В ходе исследования разработано программное обеспечение, назначением которого является внесение сокрытого сообщения в аудиофайл переменного размера методом LSB. Также продукт должен проводить корреляционный анализ стего-файла и контейнера. Вышеуказанные функции реализованы с помощью пакета MATLAB R2018b с представлением данных в оконных формах Visual Studio. На рисунках 1 и 2 представлены графики сигналов исходного аудиофайла и содержащего стегоконтейнер.

Основными возможностями программы являются:

– безопасное сокрытие информации в контейнере;

– извлечение информации из контейнера, с использованием ключа;

– графическое отображение информации, необходимой для сравнительного корреляционного анализа метода стеганографии – LSB.

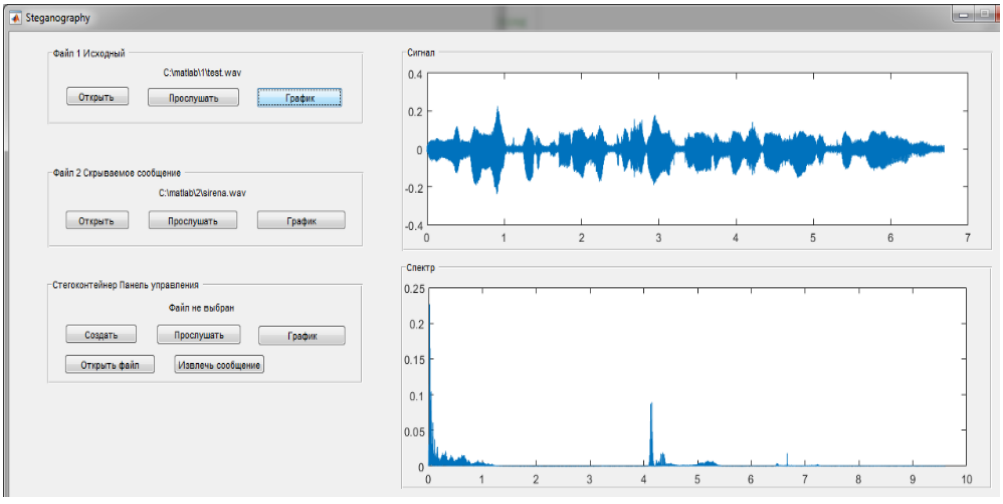


Рисунок 1 – Графики исходного (скрываемого) файла

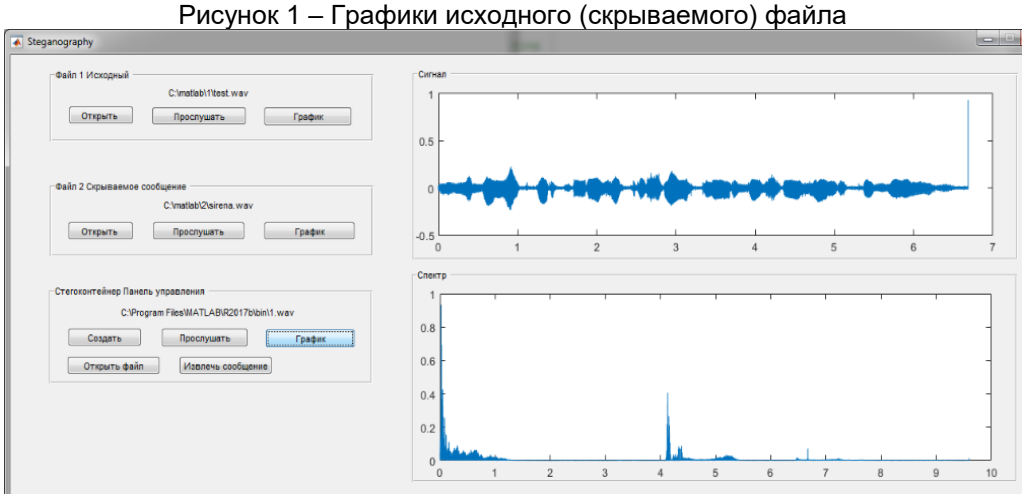


Рисунок 2 – Графики стегоконтейнера

По результатам исследования можно уверенно говорить, что человеческое ухо неспособно различить «чистый» контейнер от стего. В частотной области наибольшие расхождения между стего и контейнером находятся в области низких частот (инфразвук). Методы LSB являются неустойчивыми ко всем видам атак и могут быть использованы только при отсутствии шума в канале передачи данных.

Список использованных источников:

1 Коржик В. И. Лекции по основам стеганографии [Электронный ресурс]. – Режим доступа : www.ibts-sut.ru.

2 Конахович Г. Ф., Пузыренко А. Ю. Основы современной криптографии и стеганографии [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Стеганография#Ссылки.

3 В. Шрайбман, Стеганография аудиофайла методом LSB [Электронный ресурс]. – Режим доступа https://ru.bmstu.wiki/Стеганография_аудиофайла_методом_LSB.

4 Завьялов С. В., Ветров Ю. В, Стеганографические методы защиты информации [Электронный ресурс]. – Режим доступа : https://ghostbasenji.blogspot.com/2018/08/steganography-method-LSB.html.

ЕДИНАЯ ИДЕНТИФИКАЦИЯ ФИЗИЧЕСКИХ ЛИЦ

Шуманский Д.И.

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»
г. Минск, Республика Беларусь

Пулко Т.А. – канд. техн. наук, доцент

Система единой идентификации (СЕИ) разрабатывается с целью формирования единых подходов к обеспечению идентификации гражданина с использованием информационно-коммуникационных технологий и обеспечения юридически значимого электронного взаимодействия между гражданами и государством (за счет реализации возможности совершения юридически значимых действий посредством ЭЦП) и предназначена для предоставления информационным системам различных государственных органов и иных организаций Республики Беларусь сервиса идентификации/аутентификации. Сервисом может воспользоваться любая зарегистрированная в СЕИ информационная система. СЕИ должна предоставлять информационным системам (ИС) различных государственных органов и иных организаций Республики Беларусь сервисы аутентификации, реализованные на основе спецификации OIDC с использованием криптографических алгоритмов, определенных в государственных стандартах Республики Беларусь.

Аутентификацию может пройти любой пользователь, являющийся владельцем криптографического токена, в том числе содержащегося на идентификационной карте (КТА), или средством криптографической защиты информации, которое реализует функцию выработки ЭЦП (средство ЭЦП).

В ходе аутентификации пользователь должен выбрать средство для аутентификации, а также в качестве кого он хочет пройти процедуру аутентификации: физического лица, представителя физического лица или представителя юридического лица.

Для обеспечения аутентификации секреты аутентификации пользователя хранятся в его КТА или средстве ЭЦП. Должна обеспечиваться конфиденциальность и целостность идентификационных и других данных пользователя, передаваемых в ходе аутентификации.

СЕИ обеспечивает информационное взаимодействие ИС с информационными системами, являющимися источниками данных сервера ресурсов, посредством Общегосударственной автоматизированной информационной системы (ОАИС).

СЕИ обеспечивает централизацию процесса идентификации и аутентификации пользователей с использованием КТА или средства ЭЦП. СЕИ ведет аудит событий, связанных с выпуском, регистрацией, использованием, перевыпуском, выводом из эксплуатации билетов аутентификации (БА) и билетов доступа (БД).

СЕИ обеспечивает получение информационного запроса от ИС на получение ресурсов пользователя, определение по адресному справочнику адреса нахождения соответствующего ресурса и направление запроса через ОАИС, после получения информации из информационной системы посредством ОАИС, предоставление информации запрашивающей ИС.

СЕИ строится с использованием протокола, описанного в спецификации OpenID Connect. Для обеспечения безопасности передаваемых персональных данных и секретов аутентификации применяются криптографические алгоритмы, обеспечивающие генерацию псевдослучайной числовой последовательности, предварительное шифрование, выработку и проверку электронной ЭЦП стандартизованные в Республике Беларусь. Для выполнения протокола аутентификации и обеспечения взаимодействия с КТА и средством ЭЦП разрабатывается клиентская программа.

Список использованных источников:

1. ТР 2013/027/BY «Информационные технологии. Средства защиты информации. Информационная безопасность»
2. СТБ 34.101.21-2009 «Информационные технологии. Интерфейс обмена информацией с аппаратно-программным носителем криптографической информации (токеном)»
3. СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»
4. СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»
5. СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых»
6. СТБ 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»
9. СТБ 34.101.79-2019 «Информационные технологии и безопасность. Криптографические токены»
10. РБ.ЮСКИ.19003-01 91 01 «Профиль КТА»
11. Бердникова Ю.Н. «Белорусская интегрированная сервисно-расчетная система, как элемент электронной трансформации государственных административных процессов и услуг»
12. RFC 2616 Hypertext Transfer Protocol – HTTP/1.1
13. Спецификация OpenID Connect Core 1.0
14. RFC 2616 Hypertext Transfer Protocol -- HTTP/1.1
15. RFC 6749 The OAuth 2.0 Authorization Framework
16. RFC 6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage
17. RFC 7636 Proof Key or Code Exchange by OAuth Public Clients

ПРОГРАММНЫЙ МОДУЛЬ ВНЕДРЕНИЯ ИНФОРМАЦИИ В РАСТРОВОЕ ИЗОБРАЖЕНИЕ

Шрубиков А.Г.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Зельманский О.Б. – канд. техн. наук

Разработано программное средство на основе алгоритма LSB. Предложены способы улучшения характеристики скрытности данных, в том числе способ оптимизации используемого пространства в медиаконтейнере.

Существует множество различных методов и инструментов для защиты информации. Одним из таковых является стеганография. Стеганография – это способ сокрытия полезных данных в контейнере таким образом, чтобы неавторизованный пользователь не имел возможности обнаружить факт наличия сообщения. Под контейнером может подразумеваться текст, изображение, аудиофайлы, видеофайлы и даже неиспользуемые биты заголовков полей TCP/IP протокола [1]. Однако теме данной работы соответствует стеганография в растровых изображениях.

Существует несколько типов методов сокрытия:

– Пространственные методы. Изменения вносятся в значения пикселей таким образом, чтобы быть незаметными для человеческого глаза.

– Методы преобразования в частотной области. Более сложные методы, имеющие большую, чем в вышеописанном методе вычислительную сложность. Заключается в сокрытии информации в частотной области изображения, что, в свою очередь, повышает надёжность к различного рода атакам.

– и др.

В данной работе, был рассмотрен метод LSB из первой группы методов.

LSB (Least Significant Bit – наименее значащий бит) метод заключается в изменении младших значащих битов пикселей с целью кодирования в них секретного сообщения. Доказано, что изменение младших битов в каждом пикселе не влияет на восприятие изображения человеческим глазом [2].

Таким образом базовый алгоритм сокрытия информации может выглядеть следующим образом:

1. Преобразование секретного сообщения в массив битов.
2. Вычисление длины данного массива.
3. Преобразование длины массива в массив битов.
4. Кодирование битовой длины информационного сообщения в младших битах первых пикселей изображения.
5. Кодирование информационного сообщения в последующих битах.

Извлечение скрытой информации осуществляется обратным образом с той особенностью, что в начале требуется извлечь длину сообщения в младших битах каждого пикселя, после чего считать соответствующее количество битов.

Усложнение алгоритма может быть произведено с целью увеличения сложности раскрытия факта наличия внедрённой информации. Положительный результат может быть достигнут следующими способами:

1. Гораздо более высокую скрытность можно достичь, используя в качестве контейнера зашумлённые изображения (фотографии, отсканированные изображения) [2]. Это происходит по причине низкой закономерности используемых цветов.

2. Уменьшить вероятность несанкционированного обнаружения информации возможно благодаря непоследовательному использованию пикселей, к примеру использование каждого второго или третьего пикселя. Для оптимизации данного процесса предлагается внедрение в вышеописанный алгоритм условий, которые проверяют частное размера скрываемого сообщения и размера используемого контейнера. В результате, это значение используется для более оптимального распределения информационных битов по контейнеру. К примеру, если размер информационного сообщения меньше размера контейнера в 24 раза это означает, что для сокрытия должен использоваться младший бит составляющей синего цвета каждого пикселя. В случае если сообщение меньше контейнера в 48 либо меньше раз, возможно использование данного бита через один пиксель и т.д.

Следует упомянуть, что лучшим форматом для стеганографии данного типа является PNG, так как он использует сжатие без потерь, а также широко распространён, что позволяет избежать лишнего внимания.

Список использованных источников:

1. Kaur, H., Rani, J. A Survey on different techniques of steganography / H. Kaur, H. Rani // MATEC Web of Conferences. – 2016. – №57 – 02003.

2. Конанович, Г.Ф., Пузыренко, А.Ю. Компьютерная стеганография. Теория и практика /Г.Ф. Конанович, А.Ю. Пузыренко // «МК-Пресс» – 2006. – 288с.

ОБОСНОВАНИЕ ВЫБОРА ПЛАТФОРМЫ ДЛЯ РЕАЛИЗАЦИИ ПРИЛОЖЕНИЯ ИНТЕРНЕТ-МАГАЗИНА

Щербич А.В., Плеханова О.Е., Варламов Д.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук, доцент

Современные организации используют веб-приложения, для размещения информации, для возможности общения клиента и предпринимателя, для оплаты услуг в сети Интернет и многое другое. Но не каждая организация догадывается, что для обеспечения безопасности веб-приложения необходимо предпринимать определенные меры. Пользователи должны быть уверены в том, что информация на сайте является достоверной, их данные конфиденциальны.

По данным статистики Positive Technologie [1] в среднем на одно веб-приложение приходится 33 уязвимости, шесть из которых имеют высокий уровень риска. Число критически опасных уязвимостей, которое приходится на одно веб-приложение, по сравнению с 2017 годом выросло в 3 раза. Всё это связано с тем, что большинство разработчиков в своей работе используют открытые источники и основной задачей ставят для себя реализацию приложения, а не соблюдение комплекса мер по повышению уровня защищённости данных для разрабатываемых веб-ресурсов.

Целью работы являлась разработка веб-приложения, поддерживающего функции интернет-магазина, для последующего анализа его уязвимостей. Разработка данного приложения осуществлялась на основе ASP.NET MVC 5 Framework. Обоснования выбора платформы для реализации веб-приложения следующее:

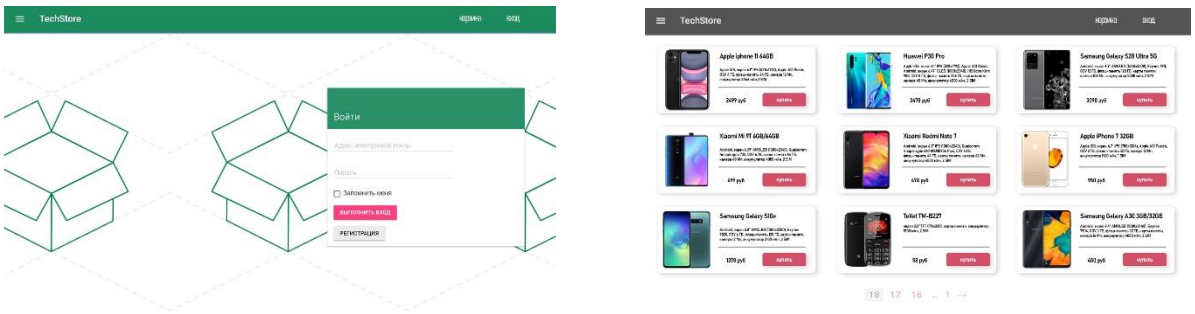
– наличие встроенных вспомогательных методов HTML, которые генерируют стандартный и понятный код разметки, что позволяет одновременно разработать графический интерфейс;

– мощная система маршрутизации URL, что позволяет вести работу с удобочитаемыми ссылками, а это в свою очередь сказывается на комфортной работе пользователя;

– структура модели MVC (Model, View, Controller), которая обеспечивает независимость компонентов друг от друга, а благодаря этому реализуется концепция разделения ответственности, что позволяет построить работу над отдельными компонентами [2].

Разработка приложения на платформе ASP.NET MVC осуществляется на языке C#, который является объектно-ориентированным. Преимущество данного языка заключается в том, что его использование позволяет создавать различные приложения, начиная с небольших программ и заканчивая крупными веб-приложениями. Также стоит отметить, что данный язык на сегодняшний день является самым распространенным в IT-отрасли, а это значит, что многие приложения написаны именно на этом языке. Таким образом, актуальным является изучение всех возможностей и уязвимостей именно данного языка, чтобы в дальнейшем позволит провести анализ уязвимостей приложений, а также составить рекомендации по их устранению. Популярность языка C# связана с тем, что у него такие же особенности как у языков Java и C++, а именно, полиморфизм, наследование, перегрузка операторов, статическая типизация и т.д. Основным достоинством языка C# является постоянное обновление, на данный момент в него добавлены такие интересные функции, как лямбда-выражения, асинхронные методы и т.д. [3].

Разработанное веб-приложение имеет стандартный набор функции, присущий интернет-магазину. Присутствует удобная форма аутентификации пользователя, а также понятный интерфейс личного кабинета. Так же есть возможность осуществления покупки с последующей оплатой и заполнением данных для доставки. Страницы авторизации пользователя и выбора товаров представлены на рисунке 1. Таким образом разработанное веб-приложение поддерживает реализацию всех действий пользователя.



а б

Рисунок 1 – Страница авторизации пользователей и электронный каталог разработанного веб-приложения интернет-магазина

Следует отметить, что разработанное приложение производит учёт действий пользователя. При регистрации новой учётной записи происходит добавление полей данных пользователя в базу данных. Также имеется пользователь администратор, которому предоставляются права изменения товаров, описания и цен. При формировании заказа происходит добавление соответствующих полей в базу данных.

В качестве языка для базы данных был выбран SQL (Structured Query Language, структурированный язык запросов), ориентированный на операции с данными в виде логически взаимосвязанных совокупностей таблиц. Особенность предложений этого языка состоит в том, что они ориентированы в большей степени на конечный результат обработки данных, чем на процедуру этой обработки [4]. Этот язык удобен тем, что сам определяет, где находятся данные, какие индексы и какие последовательности операций следует использовать для их получения.

Разработанное веб-приложение имеет две базы данных, структура которых представлена на рисунке 1. В первой базе данных (DB1) существует две таблицы: Account Info и ASPNETUSERS. В таблице ASPNETUSERS храниться информация о пользователях, среди которых поле, содержащее пароль виде хеша с использованием алгоритма MD5. В таблице Account Info хранится личная информация пользователя. Связь этих двух таблиц осуществляется на основе идентификатора поля из таблицы Account Info.

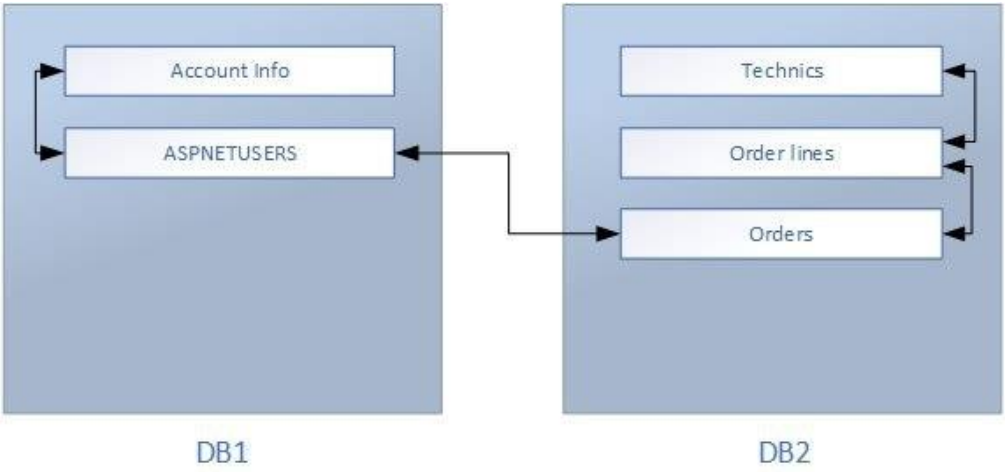


Рисунок 1 – Структура баз данных и их зависимости

Во второй базе данных (DB2) хранится три таблицы:

– Technics содержит информацию о товарах;

– OrderLines – информация о сформированном заказе;

– Orders – информация о покупателе.

Соответственно связи организуются следующим образом:

– таблицы OrderLines и Technics связываются на основе идентификатора поля таблицы Technics;

– таблицы OrderLines и Orders – на основе идентификатора поля таблицы Orders.

Для связи двух баз данных используется идентификатор поля таблицы AspNetUsers, которое передается в таблицу Orders. Выбор такой структуры баз данных обоснован необходимость отдельного хранения информации о пользователях для того, чтобы в случае несанкционированного доступа злоумышленника ко второй базе данных DB2, первая база данных DB1 была недоступной. Единственным уязвимым местом данной схемы, которое требует особого внимания, является связь двух баз данных.

Таким образом, разработанное веб-приложение для интернет-магазина включает в себя широко используемые технологии и языки программирования. В результате данное веб-приложение позволит провести исследование уязвимостей подобных интернет магазинов и написать рекомендации по их устранению.

Список использованных источников:

1. https://www.ptsecurity.com/ru-ru/research/analytics/web-application-vulnerabilities-statistics-2019/
2. https://professorweb.ru/my/ASP_NET/mvc/level1/1_2.php
3. https://metanit.com/sharp/tutorial/1.1.php
4. http://de.ifmo.ru/--books/sql/1-2.html

STRUCTURE OF LOCAL NETWORK OF IOT

Belarusian State University of Informatics and Radioelectronics
Minsk, The Republic of Belarus

THEKWT A.T

Vishnyakou U.A. – doctor of techn. science, professor

Annotation. The analysis of structure of local network of UoT are given. Some elements of such structure are discussed.

The Internet of things belongs conceptually to the next generation of networks, so its structure is similar to the well−known four layer of NGN architecture, which includes smart sensors, transport environment, services and applications [1].

The lowest level of the IoT structure consists of smart objects integrated with sensors. Sensors connect the physical and virtual (digital) worlds, providing real-time data collection and processing. Miniaturization, which reduced the physical size of hardware sensors, made it possible to integrate them directly into objects in the physical world. There are different types of sensors for the relevant purposes, for example, for measuring temperature, pressure, speed, location, etc. Sensors can have a small memory, allowing it to record a certain number of measurement results. The sensor can measure the physical parameters of the monitored object / phenomenon and convert them into a signal that can be received by the corresponding device.

Most sensors require a connection to a sensor aggregator (gateway), which can be implemented using a local area network (LAN) such as Ethernet and Wi-Fi, or a personal network (PAN) such as ZigBee, Bluetooth, and ultra-wide-band wireless communication over short distances (UWB – Ultra-Wide Band). For sensors that do not require connection to the aggregator, their connection to servers/applications can be provided using global wireless WAN networks such as GSM, GPRS, and LTE.

The large amount of data generated at the first level of IoT by miniature sensors requires a reliable and high-performance wired or wireless network infrastructure as a transport environment (network level). To implement a wide range of services and applications in IoT, it is necessary to ensure that multiple networks of different technologies and access protocols work together in a heterogeneous configuration. These networks must provide the required values for the quality of information transmission, especially for latency, bandwidth, and security. This layer consists of a converged network infrastructure that is created by integrating heterogeneous networks into a single network platform.

There are four levels of management in the IoT network: the application level; the support level for applications and services; the network level; and the device level (sensor + handler) [1].

The application and service support layer includes capabilities for various IoT objectsThe service level contains a set of information services designed to automate technological and business operations in the IoT: support for operational and business activities (OSS/BSS – Operation Support System/Business Support System), various analytical information processing (statistical, data and text mining, predictive analytics, etc.), data storage, information security, Business Rule Management (BRM), BPM – Business Process Management, etc.

At the fourth level of the IoT architecture, there are different types of applications for the relevant industrial sectors and fields of activity (energy, transport, trade, medicine, education, etc.). Applications can be "vertical" when they are specific to a particular industry, as well as "horizontal" (for example, fleet management, asset tracking, etc.), which can be used in various sectors of the economy.

The network layer includes network capabilities (access and transport network resource management, mobility management, authorization, authentication, and billing functions, AAA) and transport capabilities (providing network connectivity for transmitting IoT application information and services). The device layer includes the device's capabilities for retrieving information, preprocessing it, and gateway capabilities.

The capabilities of the device include direct exchange with the communication network, exchange through the gateway, exchange through the wireless dynamic ad-hoc network, as well as temporary stop and resume operation of the device for energy saving. The gateway features support multiple interfaces for devices (CAN bus, ZigBee, Bluetooth, Wi-Fi, etc.) and for access/transport networks (3G, LTE, DSL, etc.). Another feature of the gateway is support for protocol conversion, if the protocols of the device and network interfaces differ from each other [4].

There are also two vertical levels, the management level and the security level, covering all four horizontal levels. Vertical operational management capabilities include managing the consequences of failures, network capabilities, configuration, security, and billing data.

List of literature sources:

1. Roslyakov, A.V. Internet of things: studies. manual /A.V. Roslyakov, S. V. Vanyashin, A. Yu. Grebeshkov. – Samara, Phuthi, 2015. − 115 p.

СИСТЕМА АУТЕНТИФИКАЦИИ ДЛЯ СЕТИ ТРАНСПОРТНЫХ СРЕДСТВ

Азарко И.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Борискевич А.А. – д.т.н., профессор

Система аутентификации для сети транспортных средств основана на использовании технологии автомобильных беспроводных сетей VANET (Vehicular Ad-hoc Networks).

В VANET существует два типа связи:

– От автомобиля к автомобилю (V2V);

– Связь между транспортным средством и инфраструктурой (V2I).

Главной особенностью таких сетей является повышение эффективности безопасности дорожного движения за счет:

– Навигации;

– Информировании об ограничениях скорости;

– Предупреждение об аварийных ситуациях на дороге.

Данные таких сетей приводят к некоторым неточностям и проблемам безопасности движения транспорта, когда дело доходит до качества предобработки данных:

– Передача данных происходит только по длине маршрута, исключая требования безопасности;

– Отсутствие проверки состояния нового узла при условиях отсутствия сервера аутентификации;

– Невозможность разделения инфраструктуры.

В работе предлагается использовать алгоритм аутентификации процесса взаимоотношений участников системы аутентификации для сети транспортных средств. Алгоритм аутентификации процесса взаимоотношений участников системы аутентификации для сети транспортных средств на рисунке 1.

Рисунок 1 – Алгоритм аутентификации процесса взаимоотношений участников системы аутентификации для сети транспортных средств

Согласно рисунку 1 алгоритм аутентификации состоит из шести этапов: инициализация системы, аутентификация системы, генерация рейтинга сообщений, расчёт смещения значения доверия, выбор майнера и генерация блока, распределенный консенсус. Первый этап предлагаемого решения начинается с инициализации системы. Этот этап отвечает за проверку подлинности узлов и выдачу сертификата для них, когда узлы перемещаются в сеть. Последующим этапом является проверка подлинности системы, который действует как уровень

безопасности для аутентификации узлов, прежде чем узлы смогут начать связь друг с другом в сети. Далее, генерация рейтинга сообщений связана с предоставлением рейтинга на сообщения, отправленные узлами связи для обеспечения их надежности. После этого четвертый этап - расчет смещения значения доверия, который требуется для расчета надежности каждого узла в сети. После этого система проводит выборы майнера и блокирует генерацию, которая реализует технологию цепочки блоков для эффективного отслеживания узлов в системе. Последний этап алгоритма заключается в распределении консенсуса, который действует как бухгалтерская книга, которая распространяется по сети.

В ходе работы для программной реализации были выбраны Python и MATLAB, которые в свою очередь определили надежность данного алгоритма в сравнении с эталонным. Это связано с тем, что Python и MATLAB хорошо подходят для научного и математического программирования. Параметры для разных классификаторов были определены экспериментально.

Список использованных источников:

1. Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. Telecommun. Syst. 2012, pp.217–241

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В WI-FI СЕТЯХ

Алексеенко А.Э.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Саломатин С.Б. – канд. техн. наук, доцент

В работе рассмотрено современное состояния средств защиты информации в беспроводных сетях на основе групп протоколов IEEE 802.11, а также разработка комплекса мер для усиления безопасности на основе практических пошаговых рекомендаций.

Одной из важных задач, стоящих перед администраторами и разработчиками коммуникаций является защита беспроводных сетей по технологии групп протоколов IEEE 802.11 (Wi-Fi). В общем случае, защита должна обеспечивать невозможность доступа в сеть без разрешения администратора сети, выражаемого в выдаче кодов или специальных устройств доступа. Использование беспроводных сетей на базе протоколов IEEE 802.11 приводит к следующим особенностям защиты [1]:

1) Для подключения к беспроводной сети, не требуется физический доступ к кабелю витой пары или оптоволокну – достаточно находиться в зоне приёма сигнала маршрутизатора;

2) Передача данных по беспроводному каналу может быть перехвачена и обработана даже без устройства доступа с помощью специальных аппаратных или программных средств.

К стандартным мерам защиты относятся программные и аппаратные средства, предназначенные для решения следующих задач:

1) Предотвратить несанкционированное подключения к беспроводной сети пользователей;

2) Предотвратить доступ к запрещенным ресурсам уже подключившихся пользователей;

3) В случае проникновения, выполнить меры по сбору информации для предотвращения следующего инцидента доступа.

Для повышения уровня защиты беспроводной сети выполняются следующие меры [2]:

1) Замена ключей доступа на более комплексные;

2) Смена протоколов шифрования на более современные и устойчивые к взлому методом перебора;

3) Установка программного обеспечения для протоколирования доступа пользователей к ресурсам внутри сети.

Для администраторов беспроводных сетей, предлагается расширенный комплекс мер на основе автоматизированного контроля за доступом к сети, программируемой смены ключа доступа и перехода на последние стандарты шифрования. Комплекс предназначен для повышения всех уровней защиты беспроводной сети. Перечислим каждый шаг по усилению защиты.

На персональные компьютеры, доступ к которым осуществляется через сеть, устанавливается дополнительное «проксирующее» программное обеспечение, которое записывает в базу данных сведения о случаях доступа к ресурсам, как одобренные, так и отклоненные системой. Запись событий доступа ведется за пределы защищаемой сети, что даже в худшем случае совершенного несанкционированного доступа, позволит сохранить и расследовать историю проникновения.

Традиционным алгоритмом шифрования данных в сети Wi-Fi является WEP (Wired Equivalent Privacy) [3]. Обязательной мерой для повышения безопасности беспроводной сети является перевод всех маршрутизаторов и клиентских терминалов на протоколы шифрования данных WPA и WPA2, которые представляют собой следующее поколение алгоритмов шифрования [3].

WPA3 является преемником WPA2. WPA3 является программой сертификации и поддерживает четыре основных функции, из которых обязательна только одна: новое рукопожатие стрекозы. Эти четыре особенности следующие:

1) Новое рукопожатие под названием «стрекоза» (также называется «Одновременная аутентификация равных»), устойчивое к атакам по словарю и обеспечивающее секретность. Использует нулевые доказательства знаний.

2) Простой способ безопасного добавления устройств в сеть. Ссылка на Wi-Fi CERTIFIED Easy Connect.

3) Защитные механизмы в открытых сетях основаны на шифровании без аутентификации. Оппортунистическое беспроводное шифрование.

4) Увеличенные размеры клавиш с 192-битными ключами. Обязательно только при сертификации WPA3-Enterprise

Кроме того, WPA3 поддерживает защищенные кадры управления (PMF), что делает невозможным запуск атак отмены аутентификации. WPA2 уже поддерживает это, поэтому это не новинка WPA3. Однако с WPA PMF включаются с самого начала в программу сертификации.

Наибольший интерес в WPA3 представляет технология dragonfly (стрекоза). Dragonfly использует архитектуру клиент-сервер, где MessageManager является центральным сервером, а программные модули, которые хотели бы общаться друг с другом, являются клиентами. MessageManager поддерживает сокет прослушивания для подключения модулей и начала отправки сообщений. Все сообщения проходят через MessageManager, который перенаправляет их в подключенные модули на основании их подписок. Модули подключаются к MessageManager, подписываются на интересующие их типы сообщений, отправляют сообщения, которые будут пересылаться MessageManager всем модулям, которые подписались на эти типы сообщений, и получают сообщения, на которые они сами подписались. Модули остаются независимыми друг от друга и не должны знать, какие модули будут использовать свои сообщения или откуда поступают сообщения, которые они потребляют.

Рукопожатие стрекозы – это обмен ключами с использованием криптографии с дискретным логарифмом, которая аутентифицируется с использованием пароля или ключевой фразы. Он устойчив к активной атаке, пассивной атаке и атаке по автономному словарю.

WPA3 обладает идеальной секретностью пересылки (чего нет у WPA2) и защищает от атак методом «грубой силы» в автономном режиме.

В отличие от WPA2, WPA3 разрешено использовать только «Расширенный стандарт шифрования» (AES) и больше не использовать устаревшие протоколы, такие как «Протокол целостности временного ключа» (TKIP) или «Проводная эквивалентная конфиденциальность» (WEP).

Метод предварительного ключа (PSK) в WPA2 заменен на *одновременную аутентификацию* (SAE), которая предлагает более надежную аутентификацию на основе пароля. Сама парольная фраза больше не используется для получения ключа (ключевое слово: Pairwise Master Key (PMK)), получение ключа основано на криптографии с эллиптической кривой (ECC) или специальной форме ECC с целочисленными числами, называемыми только конечным полем.

WPA3 использует доказательство с нулевым разглашением, что гарантирует, защиту паролей при рукопожатии SAE, при этом участники рукопожатия могут быть уверены, что другая сторона знает, что они имеют такой же и правильный пароль. Рукопожатие Dragonfly по сути является протоколом SPEKE.

Помимо установки новых алгоритмов для оборудования, необходимо также усиление собственной сети за счет введения виртуальной внутренней сети, известной как технология VPN (Virtual Private Network). Создание VPN вводит дополнительное шифрование поверх уже используемых уровней, что на порядок повышает сложность взлома и делает практически невозможным силовой подбор ключей и паролей.

Также одним из способов защиты информации в Wi-Fi является автоматическая регенерация ключей доступа, производимая по расписанию и заданному алгоритму на всех устройствах доступа и клиентских терминалах. Данный способ требует разработки и установки специального программного обеспечения, которое выполняет следующие действия:

1) Создает новый ключ доступа в соответствии с правилами, заданными администратором сети;

2) Устанавливает этот ключ на все устройства, используя для подключения еще действующий предыдущий ключ;

3) Повторяет действия не реже периода, заданного администратором сети.

Ведение собственной базы ключей позволит избежать повторного использования ранее примененной последовательности, а использование аппаратно-программного генератора случайных чисел сделает создаваемый ключ непредсказуемым. При правильной настройке такого комплекса, силовой подбор ключа доступа становится практически невозможен, даже при полном доступе злоумышленника к каналу связи.

Рассмотренные меры позволяют сделать невозможным чисто силовые методы взлома беспроводной сети Wi-Fi и существенно затрудняют прочие способы, такие, как социальные и логические. Для обеспечения максимальной степени защиты, рекомендуется комбинировать предложенные меры с другими, например, контролем доступа персонала и расширенные методы идентификации пользователей с использованием электромагнитных карт или датчиков отпечатков пальцев.

Список использованных источников:

1. Пролетарский, А.В. [и др.]. Беспроводные сети Wi-Fi / А.В. Пролетарский, И.В. Баскаков, Д.Н. Чирков, Р.А. Федотов, А.В. Бобков, В.А. Платонов/ М.: Интернет-университет информационных технологий – ИНТУИТ.ру, 2013. – 216 с.

2. Пол Беделл. Сети. Беспроводные технологии. – М.: НТ Пресс, 2008. – 448 с.

3. Визавитин, О. И. Практика защиты информации в Wi-Fi сетях на основе современных программно-аппаратных средств // Молодой ученый. – 2016. – №5. – С. 182–184.

DEFENSE TOOLS IN CORPORATE INFORMATION SYSTEM, CLOUD COMPUTING AND BLOCKCHAIN

Belarusian State University of Informatics and Radioelectronics
Minsk, The Republic of Belarus

AL-MUSAWI HANI H.J., AL-ATTAR ABDULRAOUF Z.R., KHUDIER R.K.

Vishnyakou U.A. – doctor of techn. science, professor

Annotation. The analysis of tools in corporate information system, cloud computing and blockchain are given. Some elements of such as neural net, multi-agent systems are discussed.

The main sources of information about the state of corporate information system (CIS) elements that are important for the task of detecting attacks are identified: event logs and information about processes occurring on CIS servers, router logs, packets, transmitted over the network, event logs and information about processes occurring on workstations. The model of multi-agent IDS is considered, which includes a set of interacting intelligent agents, information system components, and sources of information to be analyzed for the task of detecting attacks [1].

The structure of the protected network of the CIS is presented. The server is running Slack ware Linux 10.2 with the kernel version 2.4.31. This version of the kernel is the most researched, stable, and contains the minimum number of vulnerabilities detected. The server is protected using the IPtables firewall (v1.3.3). The result of combining IDS Snort and ITU IPTables is a two-level security system: at the first level, IPTables checks the incoming packet for compliance with its filtering rules, if the packet has received permission to pass through the firewall, it is checked by the intrusion detection system for the presence of malicious code in the body of the incoming packet.

The neural networks structure using for task solving of information defense are discussed. The choice of attribute and metadata of executing files with two states (clean and with viruses) which used for multilevel perceptron teaching are built. The teaching was realized within SPSS Statistics – program of IBM Company. After the teaching of neural network the efficiently its working with the control choice of executing files was determined.

The main threats to the cloud computing (CC) environment are: virtual machine system (VMS) are dynamic, they are cloned and can «move» between physical servers, which affects the development of security integrity; CC servers and local physical clusters use the same OS and applications, which increases the «attacked surface»; when the VM is turned off, it is at risk of infection; when using CC, the network perimeter is blurred or disappears, which leads to the fact that the protection of the less secure part of the network determines the overall level of security; to protect against functional attacks, the following security measures must be used for each segment of the OV environment: for the domain controller server, effective protection against DoS attacks, for the Web server, page integrity control, for the application server, application-level screen, for the data storage system, backup, access control; most users connect to the cloud using the browser (Cross Site Scripting attacks, password theft, browser session hijacking, man-in-the-middle attacks, etc.).). A large number of VMS requires management systems that can be tampered with to block the operation of the VM; an attack on a hypervisor can lead to one VM being able to access the memory and resources of another [1].

The problem of validation. Transactions related to mechanisms for confirming authorship or authenticity using the digital equivalent of a document are used to present proof of one party to the other. The validator verifies the hash value, the transaction timestamp, and the identity of the bearer record. The mechanism for automated document validation based on the use of blockchain covers only two parties (the bearer and the verifier), which is not sufficient in the case of official documents, the issuer of which must be present in the model as a trusted third party. The confirmation model must establish not only that the document belongs to the issuer, but also confirm the issuer's authority to carry out this type of activity and additional information (for example, for the education sector, lists of training specialties for a certain period of time in accordance with the license.

The report considers the threats of IS to the CIS, and suggests using the technology of multi-agent systems to protect the perimeter of the corporate system. We consider the threats of IS for the cloud environment, and suggest using neural network technology to protect against malware that can be used in the SaaS model. The mechanisms of blockchain technology with information protection through

encryption and hashing of lists of distributed registers are considered. It is proposed to use this technology in education for document control.

List of literature sources:

1. Vishniakou, U.A. Information security in corporate systems, electronic commerce and cloud computing: methods, models, hard-software tools. Monograph / U.A. Vishniakou. – Minsk, Bestprint, 2016. – 276 p.

УПРАВЛЕНИЕ РИСКАМИ В КОРПОРАТИВНЫХ СЕТЯХ

Бабенко Ф.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ширинский В.П. – к.т.н., доцент

В работе проведен анализ основных подходов к оценке рисков информационной безопасности в корпоративных информационных сетях.

На современном этапе развития общества, когда информационную эру сменяет цифровая, глобальным трендом становится цифровизация предприятий. Технологически цифровизация базируется на масштабируемой облачной платформе и безопасной и стабильной корпоративной сети телекоммуникаций, обеспечивающей разнообразные сетевые сценарии. При этом, поскольку корпоративные сети телекоммуникаций обеспечивают технологические процессы предприятия, основным приоритетом является их надежность и информационная безопасность (ИБ) в них. Очевидно, что цифровизация предприятия может быть успешной только в том случае, если облако и сеть будут в состоянии гарантировать безопасность корпоративных данных. Вместе с тем, подключение корпоративной сети к облачной платформе, внешним сетям, использование гаджетов и электронных сервисов потенциально приводят к ее уязвимости. Все это делает проблему защиты информации и обеспечение ИБ в корпоративных сетях телекоммуникаций в целом и задачу определения рисков ИБ в этих сетях в частности крайне актуальными. При этом на первый план выходит создание быстродействующих методик как для оценки рисков ИБ в целом, так и локальных индикаторов состояния ИБ.

Информационная безопасность – это защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры. Информационная безопасность не сводится исключительно к защите информации. Поломки обслуживающей системы и задержки в ее работе также могут принести убытки.

В нашем конкретном случае под поддерживающей инфраструктурой понимается вычислительная сеть, которая, по сути, и является объектом нашего исследования. Сеть есть подвид информационной системы, безопасностью которой принято считать состояние защищённости системы, при котором обеспечивается доступность, конфиденциальность и целостность её ресурсов. В этом определении включены все три понятия, называемые «Триадой информационной безопасности»: Конфиденциальность – сохранение в секрете критичной информации, доступ к которой ограничен узким кругом пользователей (отдельных лиц или организаций). Целостность – свойство, при наличии которого информация сохраняет заранее определенные вид и качество. Доступность – такое состояние информации, когда она находится в том виде, месте и времени, которые необходимы пользователю, и в то время, когда она ему необходима.

Стоит отметить, что любая система управления ИБ ТК имеет свою техническую и организационную составляющую. Рассмотрим основную методику работы системы ИБ, применяемую в ТК на сегодняшний день. Как правило, основным техническим звеном системы управления ИБ в ТК является – подсистема ИБ, которая является органичной частью автоматизированных ИС ТК (к примеру, биллинговых). В рамках подсистемы ИБ функционируют средства защиты от несанкционированного доступа, средства криптографической защиты, средства антивирусной защиты, средства мониторинга эффективности защиты.

В рамках организационной составляющей выполняются следующие функции управления:

– организация и оперативное решение задач по защите информации;

– подбор и руководство кадрами по защите информации;

– материально-техническое обеспечение решения задач по защите информации (приобретение установка и наладка программных и технических средств защиты информации);

– контроль состояния защищенности автоматизированных ИС ТК и планирование мероприятий по защите автоматизированных ИС и развитию подсистемы ИБ;

– проведение мероприятий по повышению защищенности ИС ТК и развитию подсистем ИБ, включая управление проектами по внедрению сложных систем и проведение комплексных мероприятий по защите информации.

Задачей данной работы является разработка методов оценки риска и защищённости сетей, Для реализации потребуется следующее:

– учесть топологию сети;

– учесть параметры оборудования всех составных частей;

– учесть приоритеты и пожелания пользователя (пользователь – это тот, кто задаёт сеть, подлежащую аудиту и/или оптимизации);

– разработать математическое представление атакующих действий, их зависимостей и комбинаций;

– разработать методы вычисления риска и защищённости, а также алгоритма подбора параметров, оптимизирующих эти метрики.

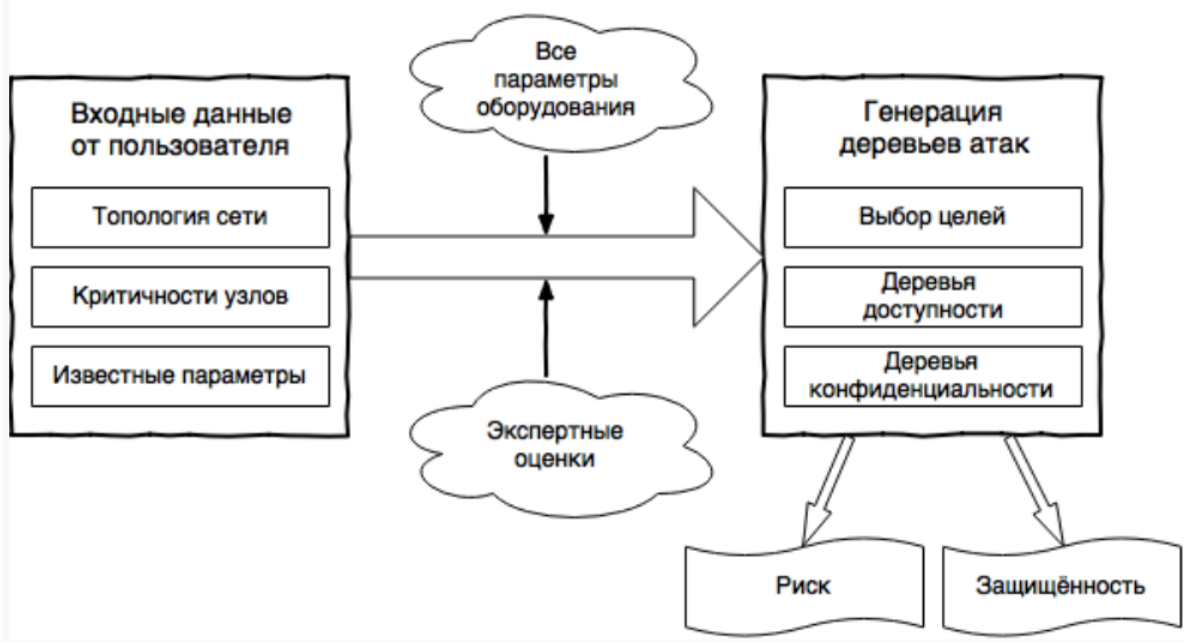


Рисунок 1 – Общая схема предлагаемого расчёта уровня риска и критичности

Список использованных источников:

1. Конеев, И.Р, Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с

2. Аникин И.В. Управление внутренними рисками информационной безопасности корпоративных информационных сетей // Научно-технические ведомости Санкт- Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2009. Т. 3. № 80. С. 35-40.

3. Аникин И.В. Метод оценки внутренних рисков информационной безопасности кор- поративных информационных сетей // Информация и безопасность. 2014. Т. 17. № 2. С. 320-323..

КЛАССИФИКАЦИЯ И СПОСОБЫ ОПИСАНИЯ ЗВЕНЬЕВ

Бобрик И.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ильинков В.А. – канд. тех. наук

На данный момент основным инструментом проектирования и разработки систем телекоммуникаций является математическое моделирование, позволяющее существенно интенсифицировать процессы анализа, синтеза, снизить материальные затраты и решить невыполнимые для других методов задачи. В статье приводится краткий обзор, классификация звеньев и методов описания линейных звеньев систем телекоммуникаций.

Классификация звеньев позволяет выработать подходы для описания звеньев различных типов в различных областях. По признаку зависимости параметров звеньев от мгновенных значений входных воздействий, звенья принято делить на:

– линейные с постоянными параметрами (инерционные, безынерционные). Активные и реактивные параметры не зависят от значений воздействий на входе и не меняются во времени;

– линейные с переменными параметрами (инерционные, безынерционные). Активные и реактивные параметры не зависят от мгновенных значений воздействий на входе, однако хотя бы один параметр изменяется во времени;

– нелинейные (инерционные, безынерционные). Хотя бы один параметр зависит от мгновенных значений входных воздействий.

Линейные звенья с постоянными и переменными параметрами обладают свойством линейной суперпозиции, поэтому к ним применимы спектральный методы моделирования и метод моделирования по формуле по формуле Дюамеля. Для нелинейных звеньев данные методы не подходят.

Описание линейных звеньев может быть во временной области, частотной, или на комплексной плоскости.

Во временной области линейное звено полностью описывается импульсной и переходной характеристиками. Импульсная характеристика представляет собой реакцию звена на дельта функцию, переходная характеристика, реакция на функцию Хевисайда.

В частотной области линейное звено описывается с помощью комплексной передаточной характеристики и амплитудно-частотной и фазо-частотной характеристики. Амплитудно-частотная характеристика представляет собой частотную зависимость отношения амплитуды реакции и амплитуды воздействия. Фазо-частотная – частотную зависимость разности фаз реакции и входного воздействия.

Описание линейного звена на комплексной плоскости производится с помощью операторной передаточной функции, которая представляет собой отношение лапласовских изображений реакции звена к воздействию. Правильное задание данной характеристики позволяет расширить возможности моделирования и упростить математическую модель.

Использование данных видов описания линейных звеньев позволяет проанализировать и синтезировать математические модели, что позволяет построить линейные звенья любой сложности с использованием минимальных затрат.

Список использованных источников:

1. Современная теория фильтров и их проектирование / под ред. Г. Темеша и С. Митра .− М.: Мир, 1977. – 500 с.

ТОКЕНЕЗАЦИЯ В NLP

Вашкевич Е.К.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Борискевич И.А. – канд. тех. наук

Обработкой естественного языка (NLP – Natural Language Processing) называется активно развивающаяся научная дисциплина, занимающаяся поиском смысла и обучением на основании текстовых данных. Токенизация – это процесс разбиения фразы, предложения, абзаца или всего текстового документа на более мелкие единицы, например, отдельные слова или термины. Каждое из этих меньших подразделений называется токенами. В статье проведен краткий обзор типов и средств токенизации.

Перед обработкой естественного языка нужно определить слова, которые составляют строку символов. В связи с этим токенизация является основным шагом для работы с **NLP**. Важность токенизации обусловлена тем, что значение текста можно легко интерпретировать, анализируя слова, присутствующие в тексте.

Пример токенизации:

"This is a cat." → ['This', 'is', 'a', cat '].

Токенизированную форму можно использовать для подсчета базовых статистик, например, количества слов в тексте или частоты слова, как необходимый шаг перед более сложными шагами обработки текста.

Существует несколько методов токенизации на языке программирования Python.

Базовым методом является токенизации (для «западных» языков, таких как русский или английский) с использованием функции Python split(). Данная функция возвращает список строк после разбиения заданной строки указанным разделителем. По умолчанию split() разбивает строку по пробелам.

Input:

text = """London of the capital of Great Britain."""

Output: [‘London’, ‘of’, ’the’, ‘capital’, ‘of’, ‘Great’, ‘Brittan.’]

Токенизация с использованием NLTK. NLTK, сокращение от Natural Language ToolKit, – это библиотека машинного обучения, написанная на Python для символьной и статистической обработки естественного языка.

NLTK содержит модуль tokenize(), который далее классифицируется на две подкатегории:

– Word tokenize: используется метод word_tokenize(), чтобы разбить предложение на токены или слова;

– Sentence tokenize: используется метод sent_tokenize(), чтобы разбить документ или абзац на предложения.

Пример работы подкатегории Word Tokenization:

Input:

from nltk.tokenize import word_tokenize

text = """London of the capital of Great Britain. It's one of the largest cities in the world."""

Output: [‘London’, ‘of’, ’the’, ‘capital’, ‘of’, ‘Great’, ‘Brittan’, ’.’, ‘It’, ’’’, ’s’, ‘one’, ‘of’, ‘the’, ‘largest’, ‘cities’, ‘in’, ‘the’, ‘world’, ’.’]

Все знаки препинания библиотека NLTK определяет, как отдельные токены.

Пример работы подкатегории Sentence Tokenization:

Input:

from nltk.tokenize import sent_tokenize

text = """London of the capital of Great Britain. It's one of the largest cities in the world."""

Output: ['London of the capital of Great Britain.', ' It's one of the largest cities in the world.']

Существуют ещё множество алгоритмов токенизации, однако библиотека NLTK – ведущая платформа для создания NLP-программ на Python. У нее достаточно легкие в использовании интерфейсы для многих языковых корпусов, имеются библиотеки для обработки текстов для классификации, токенизации и стемминга. А также это бесплатный опенсорсный проект.

Таким образом, токенизация является важным шагом в любом проекте по обработке и анализе текстов.

Список использованных источников:

1. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. – СПб.: Питер, 2018. – 480 с.: ил. – (Серия «Библиотека программиста»).

2. Боярский К. К. Введение в компьютерную лингвистику. Учебное пособие. – СПб: НИУ ИТМО, 2013. – 72 с.

3. Е.И. Большакова, Э.С. Клышинский, Д.В. Ландэ, А.А. Носков, О.В.Пескова, Е.В. Ягунова. Автоматическая обработка текстов на естественном языке и компьютерная лингвистика. – М.:МИЭМ, 2011.-272с.

СИСТЕМА ЭЛЕКТРОННОЙ СТАБИЛИЗАЦИИ ВИДЕОИЗОБРАЖЕНИЯ НА БАЗЕ ВСТРИВАЕМОГО ОДНОПЛАТНОГО КОМПЬЮТЕРА JETSON

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Горбуков А. Д.

Цветков В. Ю. – д.т.н.,доцент

На протяжении многих лет производительность процессоров увеличивалась за счет увеличения количества транзисторов на кристалле интегральной схемы и повышения тактовой частоты. Причем подобный рост происходил экспоненциально, согласно закону Мура. Однако в последние годы подобные методы увеличения производительности замедляются, давая все меньший прирост. Большинство мировых гигантов в сфере производства микропроцессоров делают ставку на параллельные вычисления, которые позволяют продолжить экспоненциальный рост производительности вычислительных устройств. Одним из популярнейших решений является использование графических процессоров. Их использование позволяет реализовывать параллельные вычисления, основанные на параллельных данных. В данной работе рассмотрена реализация алгоритма электронной стабилизации видеоизображения на базе подобного параллельного решения.

Одним из лидеров на рынке видеоускорителей является компания Nvidia. В отличии от своих конкурентов она занимает рынок не только потребительской электроники, но и серверный сегмент, а также сегмент встраиваемых решений. В частности серия компактных компьютеров Jetson основанных на SoC (System on Chip) Tegra объединяющей в себе графический процессор и центральный процессор архитектуры ARM позволяет использовать преимущество параллельных вычислений в компактных автономных системах, таких как БПЛА, роботы, автопилотируемые автомобили и автономные системы видеонаблюдения [1].

В моей работе подобный специализированный компьютер используется в БПЛА для решения комплексных задач компьютерного зрения. Одна из этих задач — это стабилизация исходного видеопотока в реальном времени. Строгие требования к весу устройства и его стоимости не позволяют полностью решить эту задачу механическими методами, такими как использование гиростабилизационной платформы. На рисунке 1 изображены графики, зависимой смещений кадров в видеопотоке по двум осям и повороту, полученных с реального видео. Не смотря на общую стабильность по различным причинам возникает высокочастотная тряска, предположительно вызванная работой двигателя и работой холодильной установки тепловизионной камеры. Подобные помехи довольно проблематично решить механическими методами без значительного увлечения веса и стоимости аппарата. Таким образом было принято решение о применении цифровой стабилизации.

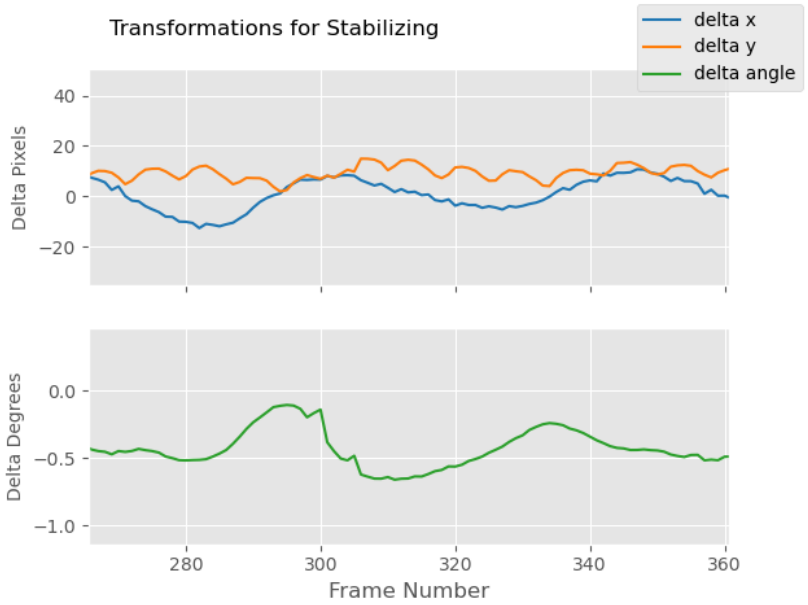


Рис. 1 – Графики зависимостей глобальных смещений кадров видеопотока.

Алгоритм цифровой стабилизации был реализован из соображений простоты и возможности задействовать мощности графического процессора. Его основой является алгоритм выделения границ, в данной реализации используется оператор Собеля, однако подобные ему операторы Прюитта и Робертса также могут применятся. Лежащая в основе данных алгоритмов операция свертки прекрасно позволяет организовать параллельные вычисления. Значения каждого пикселя

на результирующем изображении зависят только от окрестности пикселя исходного изображения, что позволяет вычислять эти значения независимо друг от друга. Т. к. графические процессоры изначально были заточены под обработку изображений, то их современные реализации содержат в себе множество дополнительных механизмов для упрощения работы с ними. В частности, механизм текстурной памяти позволяет без особых затрат со стороны программиста организовать эффективное использование L1 кэша при попиксельной параллельной обработки изображения, какой является и операция свертки.

Следующим шагом в рассматриваемом алгоритме является нахождение модуля попиксельной разности между текущим обработанным кадром и предыдущим при различных смещениях относительно друг друга. Таким образом мы сможем выбрать минимальную разность, которая будет говорить нам о том, что при данном смещении разница между кадрами минимальна, а значит с большой вероятностью камера сдвинулась именно подобным образом. В этом шаге значения разности каждого пикселя зависит только от него и от его окрестности на предыдущем кадре, таким образом подобные матрицы разности могут быть посчитаны параллельно, а потом просуммированы.

Найдя относительное смещение кадров, мы сможем построить траекторию глобального перемещения камеры. Однако, восстановленное движение содержит не только нежелательную высокочастотную составляющую, но и низкочастотную, вызванную движением летательного аппарата и камеры. Для компенсации одного типа движения и сохранения второго требуется применения высокочастотного фильтра позволяющего выделить нежелательное смещение и компенсировать его смещением кадра в итоговом видеопотоке. Т. к. разрабатываемый алгоритм должен работать в реальном времени и вызывать минимальную задержку то был выбран широко известный фильтр Калмана. При его настройке необходимо описать теоретическую модель движения нашей камеры. Тонкая настройка позволяет точно разделить нежелательные помехи в движении камеры и управляемое оператором перемещение. Подробная схема алгоритма представлена на рисунке 2.

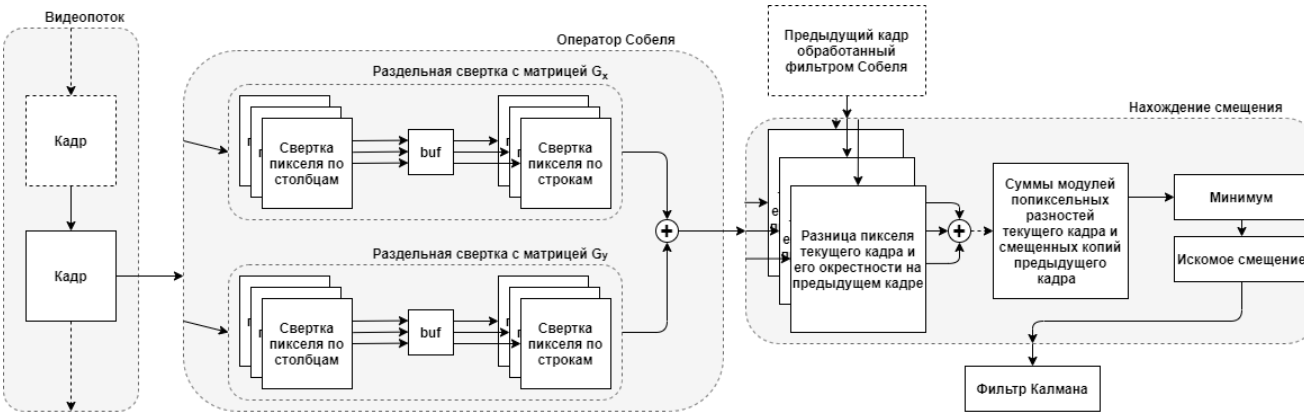


Рис. 2 – Блок-схема алгоритма.

Список использованных источников:

1. Cook, S. CUDA Programming. A Developer's Guide to Parallel Computing with GPUs / S. Cook. USA: Elsevier, 2013. – 576 p.

СИСТЕМА КОНТРОЛЯ И УЧЕТА ТРАНСПОРТА С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ СПУТНИКОВОЙ НАВИГАЦИИ И СОТОВОЙ СВЯЗИ

Денскевич С.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мищенко В.Н. – канд. тех. наук

На данный момент система контроля и учета транспорта в логистических компаниях играет важную роль, так как значительно упрощает работу и избавляет от лишних затрат. В статье излагаются теоретические основы систем навигации на основе ГЛОНАСС/GPS. Дается описание аппаратно-программной системы GPS-мониторинга транспорта.

В логистике транспорт играет значительную роль, связывая между собой отдельные экономические районы, компании, предприятия и фирмы. Перемещая материальные ресурсы и готовую продукцию из сферы производства в сферу производственного или личного потребления, транспорт тем самым участвует в производстве материальных благ. В зависимости от вида перемещаемых грузов затраты на транспортировку могут составлять более 40 % от общей стоимости этих материальных благ [1].

Современные условия ведения бизнеса ставят перед компаниями все новые и новые задачи. Сейчас для получения прибыли уже не достаточно просто составить оптимальный транспортный маршрут. Необходимо постоянно отслеживать координаты транспортных средств, чтобы динамично реагировать на быстро меняющуюся дорожную обстановку.

Развитие транспортной инфраструктуры и обеспечение навигации всех видов транспорта невозможно без современной достоверной информации об объектах поверхности Земли, которую создает и обеспечивает геодезия и картография. Эта информация очень важна для организации перевозок на всех видах транспорта, в первую очередь при решении вопроса навигационного обеспечения транспорта (практически это 80 % всего объема разработок различных навигационных систем).

Главная цель навигации заключается в непрерывном определении точного местоположения объекта в заданной системе координат и в нахождении оптимального маршрута движения этого объекта на основе получения и обработки его навигационных параметров и информации о местности, по которой он перемещается. Наиболее современные методы навигации – астрономические и радиотехнические. Астрономические методы основаны на определении положения известных небесных светил относительно выбранной системы координат. Радиотехнические методы позволяют бортовым приборам различных наземных и спутниковых навигационных систем (GPS, ГЛОНАСС, Galileo) быстро и автоматически определять и указывать местоположение, а при необходимости – и скорость, в любых погодных условиях.

Координаты, которые определяются с помощью спутниковых систем GPS, ГЛОНАСС и др., в движении могут давать точность 5…10 м. Для их улучшения существуют так называемые дифференциальные станции или пункты, на которых постоянно отслеживаются координаты и получаются поправки к ним. Эти поправки стабильны примерно на расстоянии 30…50 км, и если передать их на движущийся объект, то можно повысить точность определения координат этого объекта.

Система навигационного обеспечения представляет собой совокупность организационных, технических, программных, информационных и технологических средств, предназначенных для оперативного всепогодного, высокоточного и по возможности автономного применения навигационных и картографогеодезических средств для решения задач наземного навигационного обеспечения в режиме, близком к реальному времени.

Для анализа возможностей систем навигации рассмотрим в качестве примера разработку системы GPS-мониторинга.

Система GPS-мониторинга позволяет отслеживать на карте перемещение всех транспортных средств автопарка и наблюдать за текущим состоянием каждого из них (скорость движения, температура в рефрижераторе, открытие грузового отсека и пр.). О любом факте отклонения транспортного средства от заданных условий движения будет мгновенно сообщено пользователю системы приведено на рисунке 1, 2.

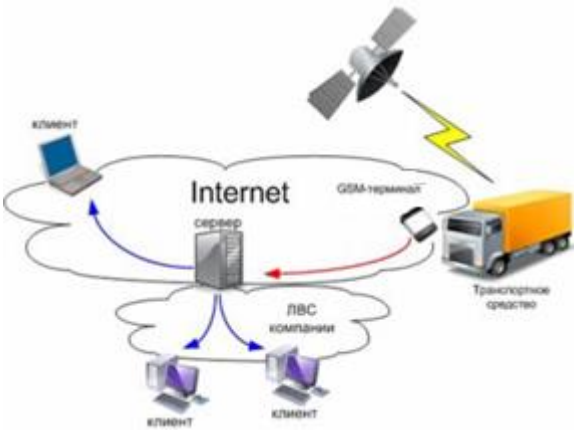


Рисунок 1 - Схема взаимодействия системы контроля и учета транспорта

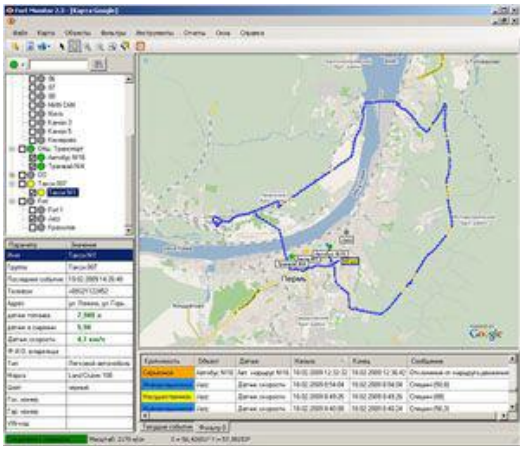


Рисунок 2 – Интерфейс программы GPS-мониторинга

Организация контроля расхода топлива поможет значительно сократить расходы за счет исключения несанкционированных сливов топлива и повышения экономичности езды водителей. Устанавливаемые на транспортное средство GSM-терминалы могут использоваться в качестве полноценной замены автомобильной сигнализации или как ее дополнение, что позволит организовать надежную многоконтурную систему охраны [2].

Система GPS-мониторинга может создавать разнообразные отчеты на основе данных, собранных о движении транспортного средства. Это отчеты о расходе топлива, пробеге, времени работы и простоев, количестве сделанных рейсов, превышениях скорости, работе специальных механизмов и пр. Координаты объекта, его скорость, высота над уровнем моря и т. п., определяются с использованием технологии GPS, остальная информация передается по GSM-терминалу. Данные, пришедшие от GSM-терминала на сервер, обрабатываются им и сохраняются в базе данных. Если покрытия GSM-сети нет, то данные накапливаются в «черном ящике» и будут переданы при появлении сети. Программное обеспечение поддерживает большое число различных форматов электронных карт, в том числе интернет-карт, загружаемых в реальном масштабе времени с серверов Google, Yahoo, Yandex и пр.

Создание системы GPS-мониторинга позволит повысить эффективность и рентабельность транспортного комплекса за счет сокращения непроизводительных пробегов и времени простоя, увеличения машино-часов на линии и сокращения затрат на содержание диспетчеров станций.

Список использованных источников:

1. Миротин Л.Б. Системный анализ в логистике: учеб. пособие/ Ы.Э. Тышбаев. - М. : Экзамен, 2004.
2. Кременец Ю.А. Технические средства организации дорожного движения. – М. : Транспорт, 1990.

ОПРЕДЕЛЕНИЕ ОРИЕНТАЦИИ И ТРАЕКТОРИИ ПЕРЕМЕЩЕНИЯ ОБЪЕКТА В ТРЕХМЕРНОМ ПРОСТРАНСТВЕ НА ОСНОВЕ СИГНАЛОВ ИНЕРЦИАЛЬНЫХ ДАТЧИКОВ

Жлобо М.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Давыдова Н.С. – канд. тех. наук, доцент

Инерциальная навигация – метод определения координат и параметров движения различных объектов (судов, самолетов, человека и др.), основанный на свойствах инерции тел. Принцип инерциальной навигации заключается в анализе движений объекта, характеризуемых изменениями во времени его ускорения, скорости и координат при помощи датчиков пространственного перемещения. Эти датчики, называемые инерциальными датчиками, лежат в основе систем инерциальной навигации (наведения), которые обеспечивают автономное измерение ускорений объекта, определение его скорости, положения в пространстве и расстояния, пройденного им от исходной точки (траектории) и, таким образом, вырабатывают навигационные данные для управления объектом[1].

В инерциальных датчиках используются подвижные массы в качестве чувствительных элементов. Такая масса под действием сил инерции, возникающих при изменении параметров движения объекта, перемещается на определенную величину, которая измеряется и преобразуется в электронный вид [2].

Основными приборами системы инерциальной навигации являются акселерометры, гироскопы и магнитометры.

Акселерометр – это прибор для измерения ускорения объекта в одном или нескольких направлениях. Акселерометр наиболее распространенного вида представляет собой чувствительную массу, связанную с корпусом пружиной. Ускорение движения объекта вызывает отклонение чувствительной массы, закрепленной на упругом шарнире, вследствие этого появляется выходной сигнал. МЭМС-акселерометры используют датчики, основанные на пьезоэффекте. В акселерометрах такого типа происходит давление грузика на пьезокристалл. Под воздействием деформации пьезоэлемент вырабатывает электрический ток. По значению деформации можно найти силу, с которой грузик давит на кристалл и, соответственно, рассчитать искомое ускорение объекта [3]

Гироскоп – это прибор для измерения угловой скорости объекта. Состоит из трёх независимых одноосных вибрационных датчиков угловой скорости, которые реагируют на вращение вокруг X-, Y-, Z- осей. Две подвешенные массы совершают колебания по противоположным осям. С появлением угловой скорости объекта происходит изменение направления вибрации, которое фиксируется емкостным датчиком. Измеряемая дифференциальная емкостная составляющая пропорциональна углу перемещения. Получившийся сигнал усиливается, демодулируется и фильтруется, давая в итоге напряжение, пропорциональное угловой скорости вращения [4].

Магнитометр представляет собой устройство для измерения интенсивности одной или нескольких составляющих магнитного поля. Чтобы определить ориентацию объекта полностью, нужен второй базисный вектор, который не будет параллелен первому, полученному из показаний акселерометра и гироскопа. Таким вектором может являться, например, вектор магнитного поля нашей планеты. Если известно его направление, то ориентация будет определена однозначно. Зная ориентацию одной системы координат относительно другой становится возможным переводить измерения из локальной системы координат устройства в глобальную. А информация об ускорениях объекта в глобальной системе координат позволят путем интегрирования восстановить скорость объекта и получить информацию об его местоположении [5].

Таким образом, основными преимуществами инерциальной навигационной системы являются компактность устройств, автономность работы и непрерывная динамическая выдача всех показаний: координат, скорости, ускорения, угловой ориентации объекта исследования.

Список использованных источников:

1. Челноков Ю.Н. Кватернионные и бикватернионные модели и методы механики твердого тела и их приложения. Геометрия и кинематика движения. – М.: ФИЗМАТЛИТ, 2006. – 512 с.
2. Бранец, В.Н. Введение в теорию бесплатформенных инерциальных навигационных систем / В.Н. Бранец, И.П. Шмыглевский. – М.:Наука, 1992. – 280с.
3. Бекмачев А. МЭМС-гироскопы и акселерометры // Компоненты и технологии. 2014. № 4.
4. Попова И.В., Лестев А.М., Семенов А.А., Иванов В.А., Ракитянский О.И., Бурцев В.А. Капсулированные микромеханические гироскопы и акселерометры для систем навигации и управления // Гироскопия и навигация. 2008. № 3.
5. Малютин Д.М. Система для определения параметров ориентации подвижного объекта по показаниям магнитных датчиков. / Малютин Д.М., Погорелов М.Г., Шведов А.П. – М. : Изд-во: Москва. Датчики и Системы: Наука, 2009. – 53-55 с.

МЕТОД ФОРМИРОВАНИЯ СЛЕДУЮЩИХ ОБРАЗОВ ОШИБОК ИЗ ПРЕДЫДУЩЕГО ПРИ ДВУМЕРНОМ КОДИРОВАНИЯ ИНФОРМАЦИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Жэнь Сюньхуань, Ма Цзюнь

Конопелько В.К. – д. т. н., профессор

В настоящее время задача исследования методов декодирования и исправления случайных ошибок помехоустойчивых кодов является актуальной, научной и прикладной задачей. В докладе рассматривается методы вычисления образов ошибок, определяется правила сокращения общего числа образов и уменьшения вычислительной сложности и повышения быстродействия.

В двумерном кодировании закодированные слова кода представляют собой таблицу, состоящую из строк слов, которые возникают в таблице и могут характеризоваться номерами строк и столбцов. Во-первых, кодируют каждые информационных символов по строкам с правилом кодирования C_1, чтобы получить закодированные проверки символы по строкам. Затем кодируют информационные биты каждого столбца в соответствии с правилом кодирования C_2, чтобы получить закодированный проверочные символы по столбцам, и, в конце концов, кодируют каждый столбец проверочных битов в соответствии с правилом кодирования C_2, чтобы получить закодированные проверочные символы, тоже являются проверочными символами по проверке. В результате получится блока (матрица $N = n_1 \times n_2$) содержатся $n_1 n_2$ символов, из которых являются $k_1 k_2$ информационными.

Сложность декодирования двумерного кодов является нахождение вектора ошибок, случайные ошибки при двумерном кодированием можно представить как образы ошибок [1] . Процедура формирования безубыточной библиотеки образов случайных ошибок сложно и трудоемко и определяется времени, затрачиваемым на вычисление библиотеки образов, и зависит от кратности ошибок. Из-за большого числа возможных ошибок соответственно имеется большие множества образов ошибок, обработка которых – сложная вычислительная задача с низким быстродействием. Поэтому их необходимо уменьшить, сделав это на предварительном этапе до обработки информации [2].

В [2] предлагала распределенный метод формирования образов ошибок, но у этого методы тратили слишком большой временной формирования общие векторы ошибок. На основе распределения идеей и выше алгоритм, дальше мы предлагаем синтетический метод формирования без избыточности образов библиотеки, которые из предыдущих образов добавления один случайный ошибочный символ – «1» и получим последующих образов.

Структура синтетического методы формирования образов от кратности $t = 2$ (предыдущих образов) получения без транспонирования образов (матрицей) $t = 3$ (последующих образов) на рисунке 1.

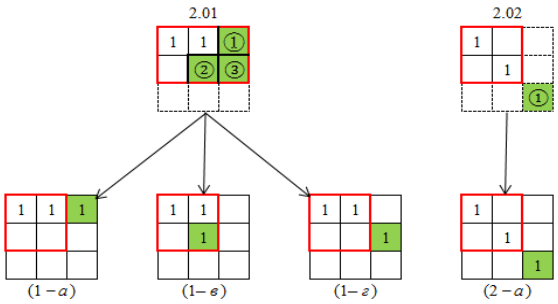


Рис. 1 - Синтетический метод формирования образов ошибок

По сравнению с известным алгоритмом синтетический метод намного раз уменьшение количества образующих образов ошибок, во первых, мы формируем образующих образов из сокращении предыдущих образов, значит не нужно анализ всех случайных образов и на много раз уменьшает вычислительную сложность; во вторых, оставление только транспонирования матрицы подмножества, также уменьшает вычислительную сложность.

Список использованных источников:

1.Конопелько В.К. Классификация векторов ошибок при двумерном кодировании информации / О.Г. Смолякова // Мн.: БГУИР 2008-7-37.С.19-28.

2.Конопелько В.К. Общие семейства в орбитальной классификации точечных образов / В.А.Липницкий., Н.В.Спичекова // Мн.:БГУИР, 2011-С.17-25.

АЛГОРИТМЫ ПОВЫШЕНИЯ РАЗРЕШЕНИЯ ИЗОБРАЖЕНИЙ

Захаренко А.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шевчук О.Г. – канд. тех. наук

На данный момент обработка изображений является актуальной и активно развивающейся областью. Благодаря увеличению разрешения улучшается не только качество восприятия человеком изображения, но и качество последующей его обработки. В статье проведен краткий обзор и классификация программных способов повышения разрешения цифровых изображений.

Увеличение масштаба и разрешения цифрового изображения дает возможность повышения его информативности. Под повышением информативности цифрового изображения понимается возможность увидеть те элементы изображения, которые не видны на кадрах низкого разрешения. Улучшение качества изображений было бы возможным путем изготовления ПЗС-матриц с большим числом фотоприемных элементов и создания на их основе новых оптоэлектронных приборов. Из-за повышения стоимости оборудования, его габаритов и прочих технических ограничений, реализация данного метода далеко не всегда является рациональной, поэтому для обработки изображений на сегодняшний день используются цифровые методы.

В зависимости от количества используемых кадров методы увеличения разрешения делятся на:

– многокадровые, которые используют несколько изображений низкого разрешения. Такой процесс реконструкции изображения высокого разрешения используется при сверхразрешении;

– однокадровые, при которых для увеличения разрешения одного изображения используется исходная информация об изображении.

Из-за отсутствия избыточности информации при обработке однокадровыми методами изображение получается более низкого качества, чем при многокадровой обработке.

Недостатки алгоритмов повышения разрешения (см. рис. 1):

– алиасинг (ступенчатость контуров, эффект «лесенки»);

– размытие;

– эффект Гиббса (ложное оконтуривания краев в виде ореолов вокруг них).

а) б) в)

Рисунок 1 – Недостатки алгоритмов масштабирования: а) алиасинг, б) размытие, в) эффект Гиббса

Однокадровые методы интерполяции можно разделить на нелиненые адаптивные и линейные неадаптивные.

Нелиненые адаптивные методы выбираются в зависимости от предмета интерполяции (резкие границы, гладкая текстура). Они применяются с целью минимизировать дефекты в тех местах, которые являются наиболее видимыми (градиентные методы, WADI, NEDI). Нелинейные методы имеют больше математических вычислений, чем линейные. Нелинейные методы позволяют избавится от артефактов, которые возникают при использовании линейных методов.

Линейные неадаптивные методы представляет собой свёртку. Эти методы обрабатывают все пиксели одинаково (метод «ближайшего соседа», билинейная интерполяция, бикубическая интерполяция и т.д.).

Благодаря тому что существует множество алгоритмов увеличения разрешения, в зависимости от поставленной задачи и исходный данных, можно подобрать наиболее оптимальный метод по повышению разрешения изображения.

Список использованных источников:

1. Yang J., Huang T. Image super-resolution: Historical overview and future challenges // Super resolution imaging. 2010. – P. 20–34.
2. Zitova B., Flusser J. Image registration methods: a survey // Image and Vision Computing, 2003. – P. 977–1000.
3. Capel D. Image Mosaicing and Super-resolution. Springer, 2004. – C.61-69.

ПАССИВНЫЕ ОПТИЧЕСКИЕ СЕТИ

Каплич А.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Урядов В.Н. – канд. тех. наук, доцент

Пассивные оптические сети (Passive Optical LAN) в инфокоммуникационной индустрии набирают популярность, они приходят на замену традиционным медным технологиям структурированной кабельной системы (СКС). Благодаря компактности, гибкой архитектуре и экономичности, технология Passive Optical LAN является предпочтительной при проектировании и установке в крупных и средних сетей в отелях, бизнес-центрах, больницах, торговых центрах, институтах и заводах.

Отличительными особенностями технологии являются:

- с помощью оптоволоконного кабеля возможно удаления устройств внутри локальной сети на несколько километров
- повышение пропускной способности сети и масштабирование, без ограничений для приложений (1G-10G-…). При этом только конечное оборудование требует замены – OLT (приемопередающий модуль) и ONT (удаленные абонентские узлы),
- гибкость проектирование пропускной способности порта,
- снижение финансовых затрат, из-за простоты проектирования и строительства сети
- снижение операционных расходов при эксплуатации, т.к. работа системы – интеллектуальная.
- Данное решение позволяет построить быструю и стабильную корпоративную сеть, соответствующую стандартам. Срок гарантии такой системы около 25 лет.

Преимуществами данной технологии являются: меньшие издержки на установку и обслуживание сети, снижение энергопотребления, небольшие площади серверных, которые необходимые для установки оборудования. Адаптацией технологии GPON является POL (Passive Optical LAN) является, используемая для строительства локальных сетей и гарантирует быструю окупаемость и низкую стоимость эксплуатации – до 50% меньше стоимости традиционной медной СКС.

Активное оборудование располагается только в серверной и около рабочих мест пользователя. Для подключения применяются проводники и различные приспособления для их организации и защиты: кабель, кабель-каналы, патч-корды, коннекторы, розетки патч-панели и т.п.

С помощью оптического одномодового волокна, технология позволяет обеспечить передачу данных, телефонии и любого типа видео на расстоянии до 20 км. Также имеется возможность использовать несколько каналов связи разных провайдеров в помещении одновременно. Это позволяет достичь ещё больший уровень безопасности соединения, т.к. поток данных шифруется на аппаратном уровне между серверной и рабочими местами.

Список использованных источников:

1. Петренко И.И, Убайдуллаев Р.Р Пассивные оптические сети PON. 2004
2. Скляров О. К. Волоконно-оптические сети и системы связи. 2010

ВЗАИМОДЕЙСТВИЕ ТЕХНОЛОГИЙ BIG DATA И INTERNET OF THINGS

Каптюг Д.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Хацкевич О.А.– канд. тех. наук

В данной работе будут подробно рассмотрены архитектура и процесс взаимодействия технологий Big Data и Internet of Things.

Архитектура IoT-системы. Типовая архитектура IIoT-систем состоит из следующих 3-х уровней:

1. Конечные устройства (Things) - датчики, сенсоры, контроллеры и прочее периферийное оборудование для измерения необходимых показателей и передачи данных в сеть по проводным или беспроводным протоколам (Serial, RS-485, MODBUS, CAN bus, OPC UA, BLE, WiFi, Bluetooth, LoRaWAN, Sigfox и пр.). Так как каждый блок данной информации небольшой по объему, такие данные называют малыми (Little Data).
2. Сетевые шлюзы и хабы (Network) - роутеры, которые объединяют и подключают конечные устройства к облаку.
3. Облако (Cloud) - удаленный сервер в датацентре, который обрабатывает, анализирует и надежно хранит информацию. Именно здесь малые данные превращаются в Big Data, когда консолидируется множество информационных потоков с различных устройств. Здесь подключаются средства анализа данных, в т.ч. с использованием методов машинного обучения (Machine Learning). Это позволяет эффективно и удаленно управлять техникой, на которой установлены конечные устройства. Например, если датчики показывают превышение допустимых значений, можно заранее спланировать профилактические меры.

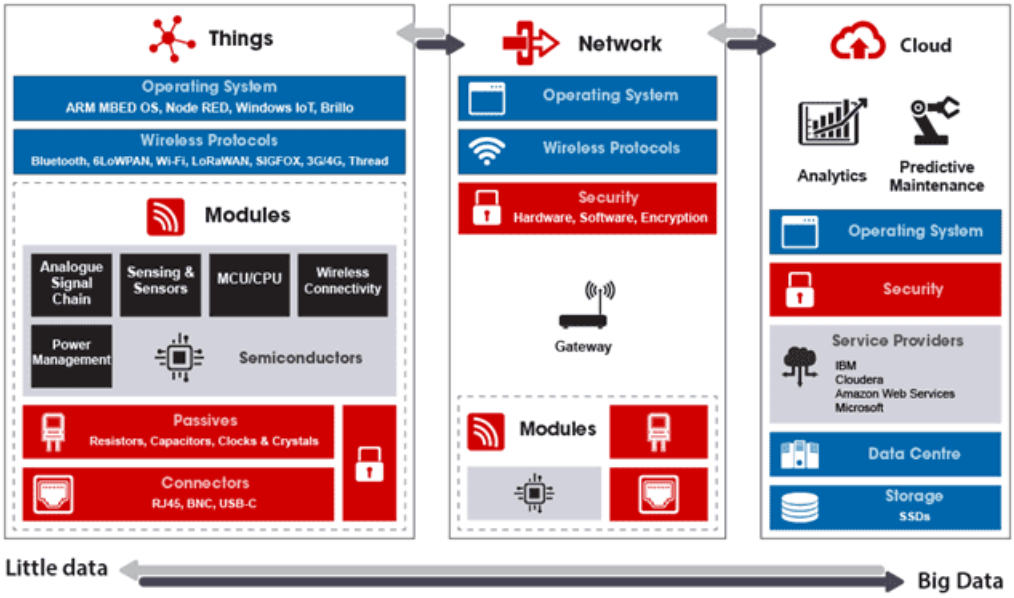


Рисунок 1 – Архитектура IoT-систем

Как работает интернет вещей с Big Data. Как правило, в промышленном IoT отсутствует прямой доступ к конечным устройствам, поэтому для соединения уровней технологического оборудования и интеллектуальных систем обработки и хранения информации используются шлюзы.

Конечные устройства являются источниками данных с низкой вычислительной мощностью, которые непрерывно передают на шлюз множество информации различного формата. Датчик конечного устройства формирует аналоговый сигнал, который преобразуется в цифровое (дискретное) значение с помощью АЦП. Это значение маркируется меткой времени и классифицируется (тегируется) локальным процессором конечного устройства. Теги могут быть простыми, состоящими из одного параметра или сложными, состоящими из нескольких

параметров. Чем сложнее тег, тем более мощным должен быть периферийный процессор и энергопотребление конечного устройства. Более информативные теги позволяют сократить количество передаваемых данных в облако и полосу пропускания информации, что в свою очередь, увеличивает скорость реакции на событие.

Шлюз, в свою очередь, отправляет данные в облачный кластер, где развернута программная IoT-платформа на базе средств Big Data для обработки и интеллектуального анализа информации. На облачном сервере данные от различных периферийных устройств интегрируются, систематизируются и анализируются с применением Machine Learning и других методов искусственного интеллекта.

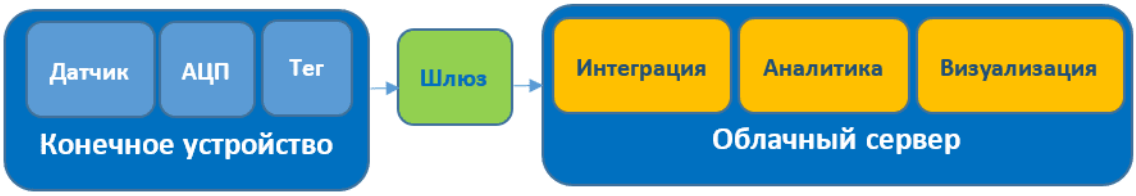


Рисунок 2 – Схема передачи информации с конечного устройства в облако

Так как, интернет вещей предполагает не только передачу информации с технологических объектов, но и удаленное управление ими, реализуется обратная связь от облачной IoT-платформы к периферийному устройству. Для этого в облаке реализуется виртуальное представление периферийного устройства, куда записывается необходимая информация по изменению его состояния, а затем передается на исполнительное устройство конечного оборудования. При этом периферийный процессор выполняет распознавание тегов и ЦАП.

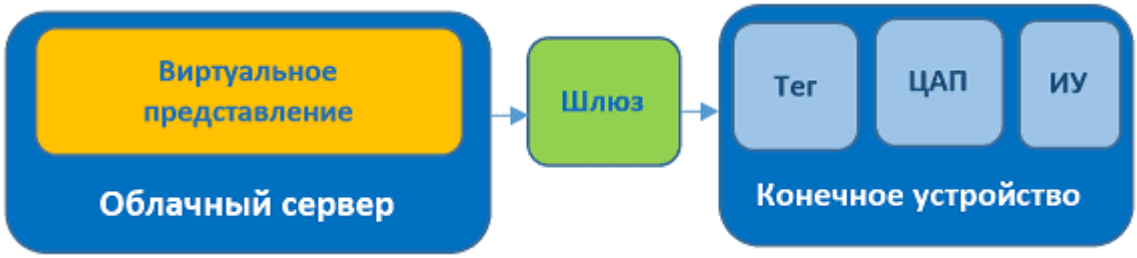


Рисунок 3 – Схема передачи данных с IoT-платформы на конечное устройство

Такая IoT-система является распределенной и масштабируемой. Однако важным моментом является надежность передачи данных. Для этого используются механизмы гарантированной доставки информации. В частности, если не удается передать данные от конечного устройства в облако или наоборот, осуществляются повторные попытки передачи. Для обмена сигналами между компонентами распределенной системы используются брокеры сообщений, которые гарантируют доставку нужных данных одному или нескольким получателям через управляемую очередь.

Список использованных источников:

1. ЭлектронныйЧто такое Big Data (BigData) в маркетинге: проблемы, алгоритмы, методы анализа [Электронный ресурс]. – Режим доступа: http://lpgenerator.ru/blog/2015/11/17/chto-takoe-big-data-bolshie-dannye-v-marketinge-problemy-algoritmy-metody-analiza/.

2. Big Data от А до Я. Часть 1: Принципы работы с большими данными, парадигма MapReduce [Электронный ресурс]. – https://habrahabr.ru/company/dca/blog/267361/.

3. Промышленный интернет вещей [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/.

СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Корякина О.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Давыдова Н.С. – к.т.н., доцент

В статье рассмотрены основные преимущества электронных документов относительно их бумажных аналогов, описана схема эффективной системы электронного документооборота. Сделан вывод о необходимости использования СЭД.

Системы электронного документооборота (далее - СЭД) стремительно внедряются в различных сферах деятельности человека. Они имеют неоспоримый ряд преимуществ перед своими бумажными аналогами: электронный архив, экономия трудовых и материальных ресурсов, однозначная идентификация документа в системе, контроль исполнителей [1]. СЭД служит основой для развертывания систем класса управления предприятием, систем управления продажами и других важных для современной организации информационных систем, поэтому от функционирования СЭД информационных систем зависит работа всей организации [2].

Предложена архитектура эффективной системы электронного документооборота (рисунок 1).

Рисунок 1 – Архитектура системы электронного документооборота

Основные функциональные возможности предложенной СЭД: 1) однократная регистрация документа, позволяющая однозначно идентифицировать документ; 2) возможность параллельного выполнения операций, позволяющая сократить время движения документов и повышения оперативности их исполнения; 3) непрерывность движения документа, позволяющая идентифицировать ответственного за исполнения документа в каждый момент времени жизни документа; 4) единая (или согласованная распределенная) база документной информации, позволяющая исключить возможность дублирования документов; 5) эффективно организованная система поиска документа, позволяющая находить документ, обладая минимальной информацией о нем; 6) развитая система отчетности по различным статусам и атрибутам документов, позволяющая контролировать движения документов по процессам документооборота и принимать управленческие решения, основываясь на данных из отчетов.

Таким образом, системы электронного документооборота влияют на эффективность работы компании в целом, помогают сократить время на обработку документов и перемещение документов между отделами и исполнителями, а также отследить маршрут документа, выставить конкретный срок исполнения для каждого сотрудника отдельно, если это необходимо.

Список использованных источников:

1. Бобылева, М.П. Эффективный документооборот: от традиционного к электронному / М.П. Бобылева. – М.: Издательство МЭИ, 2004—49 с.

2. Основные функциональные возможности систем электронного документооборота // [Электронный ресурс] – Режим доступа - https://studfile.net/preview/6862091/.

МЕТОДИКИ ОЦЕНКИ ЭКСПЛУАТАЦИОННЫХ ХАРАКТЕРИСТИК СИСТЕМ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ

Марычев Д.В., Мурашко Е.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бобов М.Н. – д.т.н., профессор

Описана необходимость существования методик оценки эксплуатационных характеристик программных и программно-аппаратных систем предотвращения вторжений как средств защиты информации в системах инфокоммуникаций.

Разработка современных технических и программных продуктов сопровождается проведением ряда тестовых исследований перед началом серийной реализации. Однако, как показывает практика, если такое тестирование выполняется впервые в процессе разработки, то оно не дает положительных результатов, на основании которых можно принять решение о готовности продукта к выпуску. Тестирование и оценка его результатов должны являться постоянной составляющей процесса формирования продукта, а не только его финальным этапом, т.е. быть частью всего жизненного цикла разработки. Каждый без исключения производитель технических средств или программного обеспечения имеет отдел специалистов по информационной безопасности, которые выполняют необходимые проверки, осуществляют контроль над защищенностью продукта и проверяют подверженность продукта уязвимостям со стороны злоумышленников.

Современные системы предотвращения вторжений являются полноценными средствами защиты информации, обязательные для внедрения в каждую инфокоммуникационную сеть, в которой передаётся и хранится информация, несущая в себе коммерческую и информационную ценность. Получение доступа злоумышленника к конфиденциальной информации может нести за собой как огромные финансовые потери, так и возможную подверженность преступникам отдельных личностей, организаций и даже стран.

Системы предотвращения вторжений (англ. Intrusion Prevention System, или IPS) являются так называемой «Системой 2 в 1», так как являются расширением систем обнаружения вторжений (англ. Intrusion Detection System, или IDS). Задача отслеживания атак у данных систем является одинаковой, однако IPS должна отслеживать активность в реальном времени и быстро реализовывать действия по предотвращению атак. Данный фактор предполагает еще больший уровень требований к системам предотвращения вторжений, так как от них непосредственно зависит безопасность и конфиденциальность различных данных.

Методики оценки эксплуатационных характеристик способствуют своевременному обнаружению проблем, которые могут привести к успешным противозаконным действиям со стороны злоумышленника. Обнаружение уязвимости на этапе тестирования позволяет разработчикам технических и программных продуктов заблокировать все возможные варианты незаконных действий злоумышленника для получения выгоды. Методики оценки позволяют определить, какие типы, виды и количество атак и других типов угроз может предотвратить тестируемая система, что позволяет распределить тестируемые системы предотвращения вторжений, как программные, так и программно-аппаратные, на определенные группы, которые предполагают сценарии их использования. а также их пригодность для использования в сетях различных организаций. Результаты грамотно определенных методик испытаний дают гарантию того, что оцененная система удовлетворяет требованиям и ведет себя в соответствии с ними во всех предусмотренных ситуациях. Также данные результаты помогают определить, какими эксплуатационными параметрами может обладать система, что позволит потенциальному покупателю, увидев заключения экспертов, определить, какое именно решение правильнее и выгоднее всего использовать в организации инфокоммуникационной система.

Для того, чтобы стандартизовать эту деятельность, научное и профессиональное сообщества находятся в постоянном сотрудничестве, направленном на выработку базовой методологии, политик и индустриальных стандартов в области технических мер защиты информации, юридической ответственности, а также стандартов обучения пользователей и администраторов. Эта стандартизация в значительной мере развивается под влиянием широкого спектра законодательных и нормативных актов, которые регулируют способы доступа, обработки, хранения и передачи данных, но подразумевает собой засекречивание методик испытаний, чтобы исключить доступ к этой информации потенциальным злоумышленникам.

АЛГОРИТМ СКЕЛЕТИЗАЦИИ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ОРТА И ZHANG-SUEN

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ма Цзюнь, Жэнь Сюньхуань

Конопелько В.К. – д. т. н., профессор

В настоящее время задача исследования и разработки методов скелетизации бинарных изображений является актуальной задачей, научной и прикладной. Наиболее актуальной она является в условиях ограниченных вычислительных и временных ресурсов.

Скелетизация обеспечивает представление бинарного изображения в виде множества тонких линий, взаимное расположение, размеры и форма которых адекватно описывают размеры, формы и ориентации в пространстве соответствующих областей изображения. Наиболее высокое качество скелетов обеспечивают итерационные параллельные алгоритмы. Они могут реализовываться с использованием одной или нескольких подитераций, на каждой из которых происходит удаление избыточных элементов, окрестности которых удовлетворяют определенным условиям. Для многих одноподитерационных алгоритмов характерно нарушение связности и формирование избыточных фрагментов скелета. Наиболее качественные скелеты формирует известный одноподитерационный алгоритм ОРТА, основанный на 18-ти бинарных масках, но он чувствителен к контурному шуму и имеет высокую вычислительную сложность. Благодаря относительной простоте широкую известность получил двухподитерационный алгоритм Zhang и Suen (ZS), основанный на 6-ти логических условиях, но он размывает диагональные линии толщиной 2 пикселя и удаляет области размером 2x2 пикселя. Оба алгоритма не обеспечивают достижение минимальной толщины линий скелета [1-2].

В задачах параметризации объектов изображений часто используется скелетизация (утончение) – преобразование однородной области, соответствующей объекту, во множество тонких линий, взаимное расположение, размеры и форма которых передает информацию о размере, форме и ориентации в пространстве соответствующей области.

В параллельных алгоритмах порядок обработки пикселей на каждой итерации не влияет на результат, что обеспечивает стабильность скелета при повороте изображения и позволяет повысить скорость скелетизации за счет распараллеливания вычислений. Для построения предельно тонких связанных скелетов бинарных изображений с низкой вычислительной сложностью предложен алгоритм модифицированного одноподитерационной скелетизации на основе комбинации и упрощения моделей одноподитерационной ОРТА и двухподитерационной ZS скелетизации. Предлагаемый алгоритм отличаются:

а) от ОРТА исключением масок, предназначенных для удаления избыточных элементов на горизонтальных и вертикальных прямых линиях скелета, использованием упрощенного условия для удаления пикселей в точках изломов линий скелета, исключением предназначенных для удаления избыточных концевых элементов скелета;

б) от ZS исключением всех условий удаления пикселей, кроме двух. Данные отличия позволили уменьшить толщину скелета, повысить скорость скелетизации, восстанавливаемость исходного изображения по скелету, снизить избыточность связей элементов скелета.

Алгоритм ОРТА включает в себя 4 основные части: модуль поиска, модуль проверки подключения, модуль коррекции одного пикселя и модуль удаления контурной точки.

Структура модифицированного алгоритма скелетизации представлена на рисунке 1.

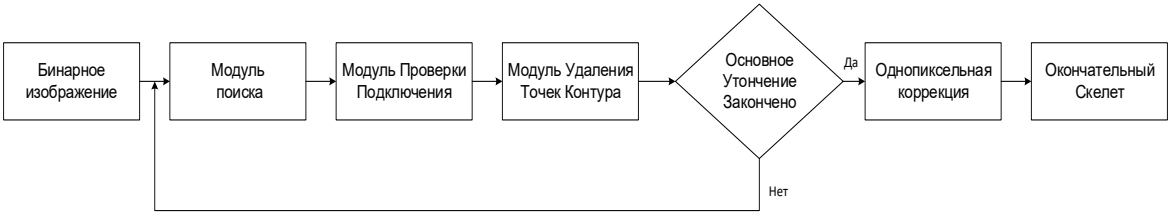


Рис. 1 - Структура модифицированного алгоритма скелетизации

По сравнению с ОРТА и ZS алгоритм модифицированный алгоритм обеспечивает уменьшение толщины скелета, повышение скорости скелетизации, повышение восстанавливаемости исходного изображения по скелету и уменьшение избыточности связей между пикселями скелета.

Список использованных источников:
1. Zhang T.Y. A fast parallel algorithm for thinning digital patterns / C.Y. Suen . – 1984. №3 – С.236-239.

2. Boudaoud L.B. A new thinning algorithm for binary images / A. Sideю., A. Tari. – 2015. – С.1-6.

ОПРЕДЕЛЕНИЕ КОЖНЫХ ЗАБОЛЕВАНИЙ ПО ФОТОГРАФИИ ПРИ ПОМОЩИ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Медведев Е.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Борискевич И.А. – канд. тех. наук, доцент

Рак является основной причиной смерти во всем мире. Как исследователи, так и врачи сталкиваются с проблемами борьбы с раком. По данным Американского онкологического общества, в 2019 году ожидается 96 480 смертей от рака кожи, 142 670 от рака легких, 42 260 от рака молочной железы, 31 620 от рака простаты и 17 760 смертей от рака головного мозга в 2019 году (Американское онкологическое общество, новый отчет о раковых заболеваниях, 2019 год). Раннее выявление рака является главным приоритетом для спасения жизни многих людей. Как правило, визуальный осмотр и ручные методы используются для диагностики рака. Такая ручная интерпретация медицинских изображений требует больших затрат времени и очень подвержена ошибкам.

По этой причине в начале 1980-х годов были внедрены системы компьютерной диагностики (CAD), чтобы помочь врачам повысить эффективность интерпретации медицинских изображений. Для еще большего повышения эффективности данных методов можно использовать искусственные нейронные сети.

Этапы диагностики рака:

1. Предварительная обработка
2. Сегментация изображения
3. Постобработка
4. ABCD-Правило
5. Метод из семи пунктов
6. Метод Мензиса
7. Анализ паттернов

Также в исследовательской работе присутствует обзор искусственных нейронных сетей, которые могут использоваться для решения задачи диагностики кожных заболеваний:

1. Сверточные нейронные сети (CNN)
2. Многомасштабная сверточная нейронная сеть (M-CNN)
3. Сверточная нейронная сеть с многоэлементным обучением (MIL-CNN)
4. Полностью сверточные сети (FCN)
5. Рекуррентные нейронные сети (RNN)
6. Долгосрочная кратковременная память (LTSM)
7. Ограниченная машина Больцмана (RBM)
8. Автоэнкодеры (AEs)
9. Сложенные автоэнкодеры
10. Разреженные автоэнкодеры SAE
11. Сверточные автоэнкодеры CAE
12. Сети глубокого убеждения (DBN)
13. Нейронная сеть адаптивного нечеткого вывода (AFINN)

Список использованных источников:

1. Torre, L.A.; Bray, F.; Siegel, R.L.; Ferlay, J.; Lortet-Tieulent, J.; Jemal, A. Global cancer statistics, 2012. *CA Cancer J. Clin.* **2015**, *65*, 87–108.
2. Siegel, R.L.; Miler, K.D.; Jemal, A. Cancer Statistics, 2016. *CA Cancer J. Clin.* **2016**, *66*, 7–30. [CrossRef] [PubMed]
3. Tian,Z.;Liu,L.;Zhang,Z.;Fei,B.PSNet:ProstatesegmentationonMRIbasedonaconvolutionalneural network. *J. Med. Imaging* **2018**, *5*, 021208. [CrossRef]
4. Zhang,X.;Wang,S.;Liu,J.;Tao,C.Towardsimprovingdiagnosisofskindiseasesbycombiningdeepneural network and human knowledge. *BMC Med. Inform. Decis. Mak.* **2018**, *18*, 59. [CrossRef]
5. Rezvantalab,A.;Safigholi,H.;Karimijeshni,S.Dermatologistleveldermoscopyskincancerclassification using different deep learning convolutional neural networks algorithms. *arXiv* **2018**, arXiv:1810.10348.

МЕЖСАЙТОВЫЕ АТАКИ С ВНЕДРЕНИЕМ СЦЕНАРИЯ (XSS)

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

А.С. Михайлов

Саломатин С.Б. – канд. техн. наук

Рассмотрено вопросы, связанные незаконное использование JavaScript, правила безопасности, чтобы предотвратить возможную XSS атаку, и предоставлено собственное исследование, связанное с проверкой сайтов на наличие организованной безопасности веб-сайтов.

Введение

Во время межсайтовой атаки с внедрением сценария (XSS) атакующая сторона внедряет в легальную Web-страницу вредоносный код, который затем запускает вредоносный сценарий на стороне клиента. При посещении пользователем зараженной страницы сценарий загружается в браузер пользователя и там запускается. Эта схема имеет множество разновидностей. Вредоносный сценарий может получать доступ к cookie-файлам браузера, сеансовым маркерам или другой чувствительной информации, хранящейся в браузере. Межсайтовый скриптинг (XSS) — пожалуй, самый типичный вид уязвимостей, широко распространённых в веб-приложениях. По статистике, около 65 % сайтов в той или иной форме уязвимы для XSS-атак.

Цель работы состоит в разработке и исследовании программ защиты информации от межсайтового скриптинга.

1. Межсайтовые атаки с внедрением сценария

Рассматриваются следующие схемы возможные атаки в рамках схемы работы межсайтовой атаки с внедрением сценария.

Хранимые XSS (постоянные) - один из самых опасных типов уязвимостей, так как позволяет злоумышленнику получить доступ к серверу и уже с него управлять вредоносным кодом (удалять, модифицировать).

Отраженные XSS (непостоянные) - в этом случае вредоносная строчка выступает в роли запроса жертвы к зараженному веб-сайту.

DOM-модели - в этом варианте возможно использование как хранимых XSS, так и отраженных. Суть заключается в следующем: злоумышленник создает URL-адрес, который заранее содержит вредоносный код, и отправляет его по электронной почте или любым другим способом пользователю, человек переходит по этой ссылке, зараженный сайт принимает запрос, исключая вредоносную строку, на странице у пользователя выполняется сценарий, в результате чего загружается вредоносный скрипт и злоумышленник получает cookies.

2. Правила безопасности

Защититься от XSS возможно, но защита должна применяться последовательно, без исключений и упрощений, желательно с самого начала разработки веб-приложения. Внедрение защиты на более поздних этапах может быть дорогостоящим делом.

Проверка входных данных. Проверка ввода — только первая линия защиты веб-приложения. При таком типе защиты мы знаем лишь то, как сейчас используются ненадёжные данные, и на этапе получения данных не можем предсказать, где и как они будут дальше применяться. Сюда относятся практически все текстовые данные, так как мы всегда должны обеспечивать пользователю возможность написания кавычек, угловых скобок и других символов.

Проверка работает лучше всего благодаря предотвращению XSS-атак на данные, которым присущи предельные значения. Допустим, целое число не должно содержать специфические для HTML символы. Параметры, такие как название страны, должны соответствовать заранее заданному списку реальных стран, и т. д.

Проверка входных данных помогает контролировать данные с определённым синтаксисом. Например, допустимый URL-адрес должен начинаться с префикса http:// или https://, а не с гораздо более опасных конструкций javascript: или data:. По сути, все адреса, полученные из непроверенных входных данных, должны проверяться на наличие этих тегов. Экранирование URI

javascript: или data: имеет такой же эффект, как экранирование легального URL-адреса. То есть вообще никакого эффекта.

Хотя проверка входных данных не может блокировать всю зловредную полезную нагрузку при XSS-атаке, она способна остановить наиболее очевидные типы атаки.

Экранирование (а также кодирование). Экранирование данных на выходе позволяет гарантировать, что данные не будут ошибочно восприняты принимающим парсером или интерпретатором. Очевидные примеры — знаки «меньше» и «больше», которые обозначают HTML-теги. Если позволить этим символам быть вставленными из ненадёжных входных данные, злоумышленник сможет вводить новые теги, которые браузер будет отрисовывать. Обычно эти символы заменяются последовательностями > и $lt;.

Замена символов предполагает сохранение смысла экранированных данных. Экранирование просто заменяет символы, имеющие определённое значение, альтернативными. Обычно используется шестнадцатеричное представление или что-то более читабельное, например, HTML-последовательности (если их применение безопасно).

Способ экранирования зависит от того, какого типа содержимое внедряется. Экранирование HTML-кода отличается от экранирования JavaScript, которое, в свою очередь, отличается от экранирования адресов. Применение неверной экранирующей стратегии для определённого контекста способно привести к неэффективности защиты, к созданию уязвимости, которой может воспользоваться злоумышленник.

Заключение

Разработанные алгоритмы, реализованные в виде программы позволяют повысить эффективность защиты веб-приложения от атак. Они значительно упрощают процесс тестирования веб-ресурса разработчиком, благодаря функционалу формирования отчета с рекомендациями по устранению найденных уязвимостей.

Список литературы

1. Элхади А.М. Полное пособие по межсайтовому скриптингу // [Электронный ресурс].
2. Элхади А.М. Уязвимости веб-приложений: пора анализировать исходный код // [Электронный ресурс].
3. Джатана Н., Агравал А., Собти.К. Пост эксплуатация XSS: продвинутые методы и способы защиты// [Электронный ресурс].

СИМУЛЯТОР СЕТЕВЫХ ТРАНСПОРТНЫХ КОММУНИКАЦИЙ SUMO

Белорусский государственный университет
информатики и радиоэлектроники
г. Минск, Республика Беларусь,

П.А. Москалев

М.Ю. Хоменок

Рассматриваются особенности модульной структуры симулятора SUMO, пользовательских интерфейсов и основные возможности выполнения исследований сценариев движения сетевых узлов.

Симулятор SUMO – Simulation of Urban MObility представляет собой дискретно-временную платформу для моделирования транспортных потоков и предназначен для оценки моделей мобильности транспортных средств в контексте организации дорожного движения, имитационной оценки систем видеонаблюдения за дорожным движением, ориентированной на прогнозирование способности разработанной системы наблюдения удовлетворять поставленным задачам при предполагаемой скорости распознания и/или оснащения транспортных средств, а также транспортных коммуникаций V2V (Vehicle to Vehicle) и V2I (Vehicle-to-Infrastructure) с учетом картографических особенностей области моделирования [1].

SUMO-это открытый, портативный пакет имитационного, предназначенный для работы с большими дорожными сетями. Он в основном представлен разработками сотрудниками Института транспортных систем при германском Аэрокосмическом центре.

Его реализация началась в 2001 году, а первый выпуск программного обеспечения с открытым исходным кодом в 2002 году под лицензией GNU public license (GPL).

Основной задачей было поддержать исследования по моделирования трафика с помощью бесплатного инструмента, в котором могут быть реализованы собственные алгоритмы моделирования трафика с учетом изменений сетевой инфраструктуры. В комплекте есть множество вспомогательных инструментов, которые обрабатывают такие задачи, как поиск маршрута, визуализация, импорт и расчет параметров сети, и различные пользовательские интерфейсы API (application programming interface) для удаленного управления имитацией.

С точки зрения инфокоммуникационных технологий SUMO помогает отследить взаимодействие транспорта, установку соединений между передвигающимися в городской черте автономными модулями связи, построение различного типа сетей, обмен данными между модулями [2].

Транспортные сети в SUMO могут быть созданы либо с помощью приложения под названием “ netgenerate ", либо с помощью импорта цифровой дорожной карты, рис.1. Импортер дорожной сети "netconvert" позволяет также считывать сети с других симуляторов движения, таких как VISUM, Vissim или MATsim.

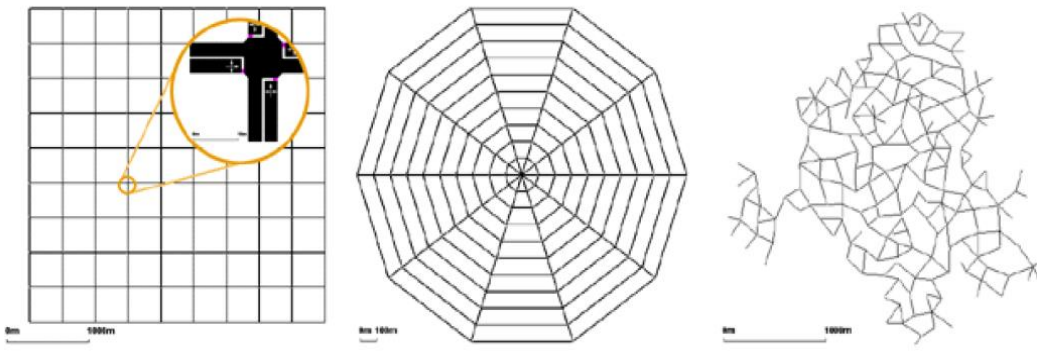


Рис.1 – Примеры топологии транспортных сетей, построенных приложением “ netgenerate ". Слева направо: “manhattan”, “spider”, “random network”.

Каждое транспортное средство задается идентификатором, временем отправления и маршрутом движения по сети. При необходимости каждое транспортное средство можно описать более подробно, указывая, например, используемую дорожную полосу движения, скорость и другие параметры автомобиля и параметры движения. Маршруты обычно рассчитываются путем

определения моделей трафика и маршрутизации с учетом вычисления кратчайшего пути в рамках различных функций затрат.

Рис.2 – Выборка моделируемого участка картографической области в OSMWebWithard

Высокая агрегация с такими приложениями, как NETSIM, NS3, Wireshark – позволяют оценивать эффективность применяемых технологий, качество соединения, правильность размещения узлов, напряженность трафика в узлах при разных уровнях загруженности дорог. При этом имеется возможность загружать реальные участки дорог, при помощи модуля OSMWebWithard, рис.2.

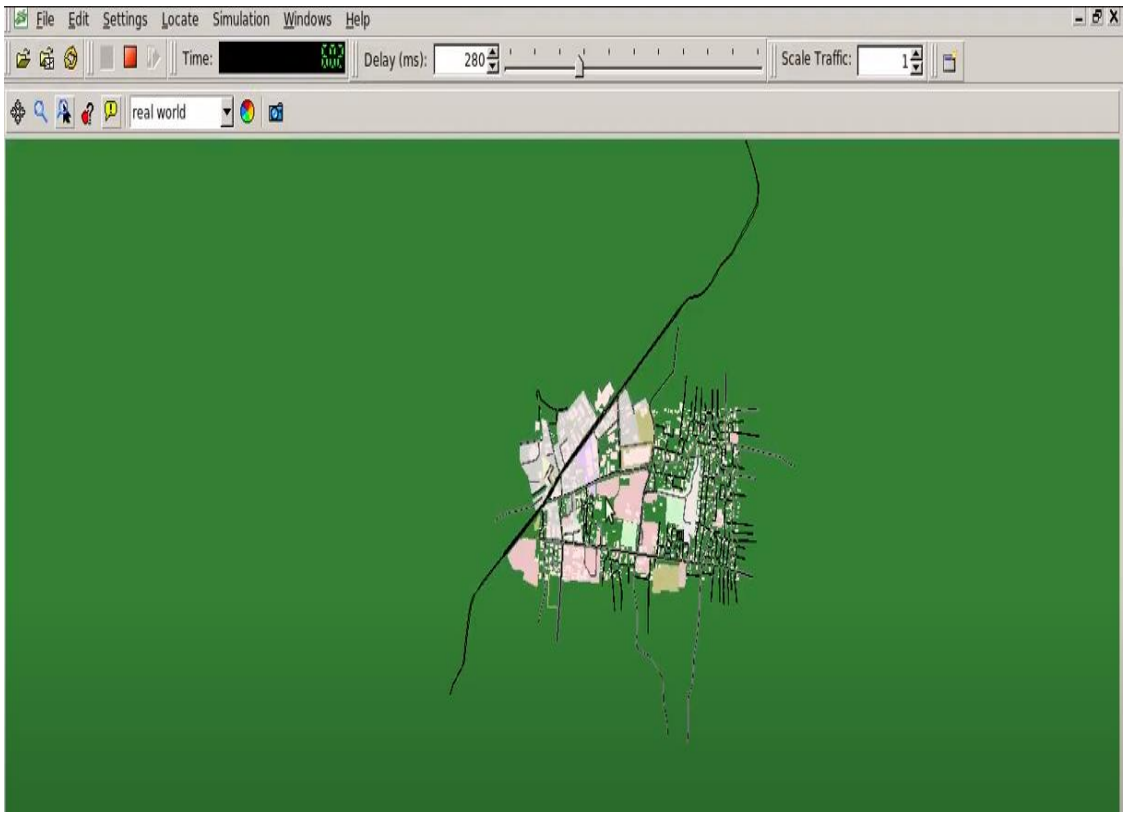


Рис.3 – Конвертация моделируемого участка картографической области в SUMO

Пример частного применения демонстрируется на рисунке 3, где выбранный участок дороги в OSMWebWithard путем симуляции карты переносится в SUMO. В ней задаются параметры и создается симуляция движения автономных модулей. Данные о перемещениях модулей передаются в NS3, обрабатываются и создаются отчеты, используемые в WireShark для оценки трафика модулей, рис.4.

Платформа моделирования SUMO предлагает множество функций:

- Поддерживаемые форматы импорта: OpenStreetMap, VISUM, VISSIM, NavTeq.

- Приложение “ netedit " позволяет графически редактировать дорожные сети.

● Интерактивное взаимодействие и управление симуляцией через интерфейс управления трафиком TraCI (Traffic Control Interface), который позволяет использовать SUMO в комбинации со связными симуляторами, такими как ns2 и ns3, для моделирования сетей по технологии Vanet.

● Моделирование транспортных потоков для мультимодальных перевозок, например транспортных средств, общественного транспорта и пешеходов и др.

● Расписание работы светофоров или алгоритмов для их адаптации к текущему трафику может быть импортировано или сгенерировано SUMO автоматически.

● Отсутствие искусственных ограничений в размере сети и количестве смоделированных транспортных средств.

● Сумо реализован на языке C++ и использует только портативные библиотеки.

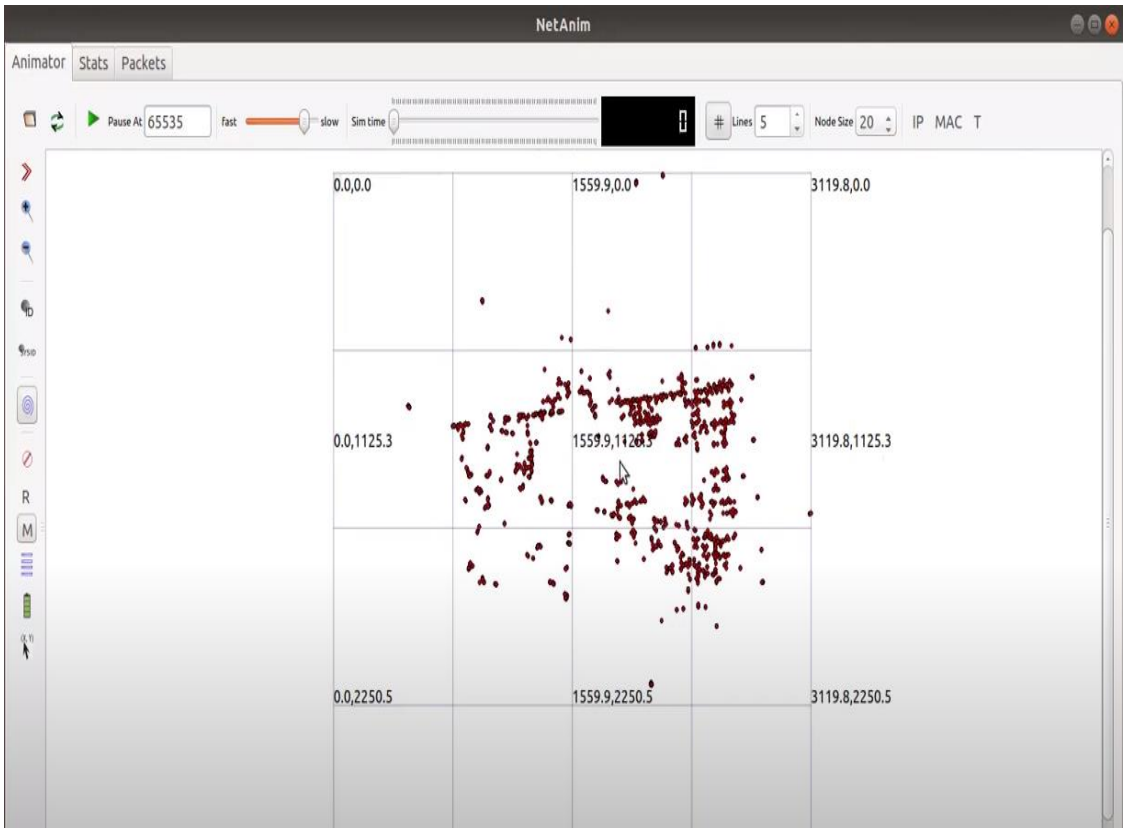


Рис.4 – Симуляция сетевой топологии в NetAnim

Список используемых источников:

1. Определения и принципы действия SUMO [Электронный ресурс]. – Режим доступа: http://sumo.sourceforge.net/.
2. Аггрегируемость, настройка, модули [Электронный ресурс]. – Режим доступа: https://www.nsnam.org/.
3. Применение SUMO. [Электронный ресурс]. – Режим доступа: https://www.dlr.de/ts/en/desktopdefault.aspx/tabid-9883/16931_read-41000/

СЕТЕВЫЕ ТРАНСПОРТНЫЕ КОММУНИКАЦИИ VANET

Белорусский государственный университет
информатики и радиоэлектроники
г. Минск, Республика Беларусь,

П.А. Москалев

М.Ю. Хоменок

Аннотация. Анализируются основные аспекты исследований, связанных с реализацией автомобильных сетей с самоорганизующейся топологией, создаваемых в рамках концепции интернета вещей IoT, с целью создания инфокоммуникационной структуры для участников дорожного движения.

Автомобильные сети VANET (Vehicular Ad Hoc Network), соответствующие концепции ITS ((Intelligent Transport System), интегрируют сети Ad-Hoc с самоорганизующейся топологией, беспроводные локальные сети (WLAN) и сети сотовой связи (Cellular Telecommunication) и нацелены на достижения интеллектуальных межтранспортных коммуникаций и повышения безопасности и эффективности дорожного движения [1].

В этих сетях транспортные средства взаимодействуют друг с другом и, возможно, с придорожной инфраструктурой, чтобы обеспечить доступ к информационным сервисам, варьирующихся от безопасности до помощи водителю и доступа в интернет к конкретной контекстной информации (например, об условиях движения, обновления услуг, планировании маршрута) и предоставления мультимедийных услуг (VoIP, instant messaging и т.д.), рис.1.

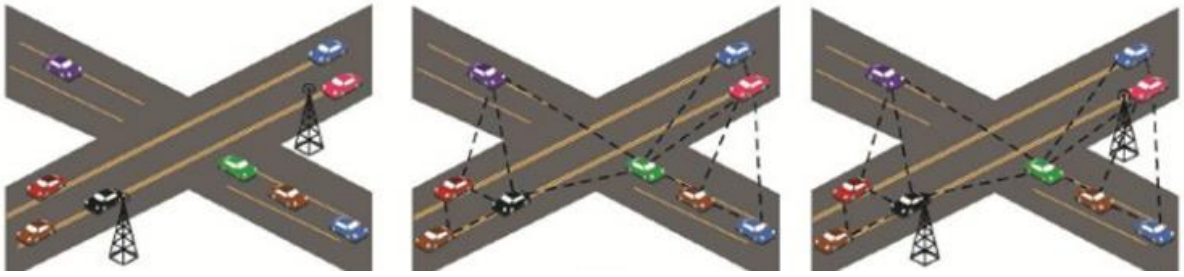


Рис.1 – Сетевая архитектура Vanet: слева направо – взаимодействие через базовые станции сотовой связи, взаимодействие через узлы транспортных средств, взаимодействие с узлами транспортных средств и объектами дорожной инфраструктуры (гибридная архитектура).

В этих сетях знание положения узлов в реальном времени является предположением, которое должна учитываться используемыми протоколами маршрутизации и приложениями. Сети VANET отличаются от других видов Ad-Hoc сетей гибридной сетевой архитектурой, характеристиками движения узлов и сценариями решаемых задач.

Основными сложностями данной технологии являются работа на высоких скоростях и в условиях препятствий для прохождения сигнала, что требует быстродействия принятия решений. В противном случае на скоростях в 100 и более километров в час при встречном движении сигнал сильно искажается, а часть информации может теряться. Так на скорости в 100 километров в час автомобиль преодолевает примерно 30 метров в секунду. Соответственно при встречном движении скорость сближения автомобилей – 60 метров в секунду. Дальность действия обычного Wi-Fi роутера – приблизительно 150 метров. При условии, что соединение установилось моментально, что реально не достигается, водителю для корректировки остается 2.5 секунды. Добавляя скорость установки соединения, скорость реакции водителя, инерционность автомобиля, шумы от рельефа и метеорологических условий, результат намного превышает 2.5 секунды.

Основные вопросы реализации интеллектуальных транспортных сетей и беспроводного доступа в автомобильном окружении представлены в рекомендациях IEEE 1609, концепция WAVE (Wireless Access in Vehicular Environments) [2].

Технология VANET использует стек протоколов IEEE 802.11p WLAN с частотой работы в районе 5.9 GHz, рис.2.

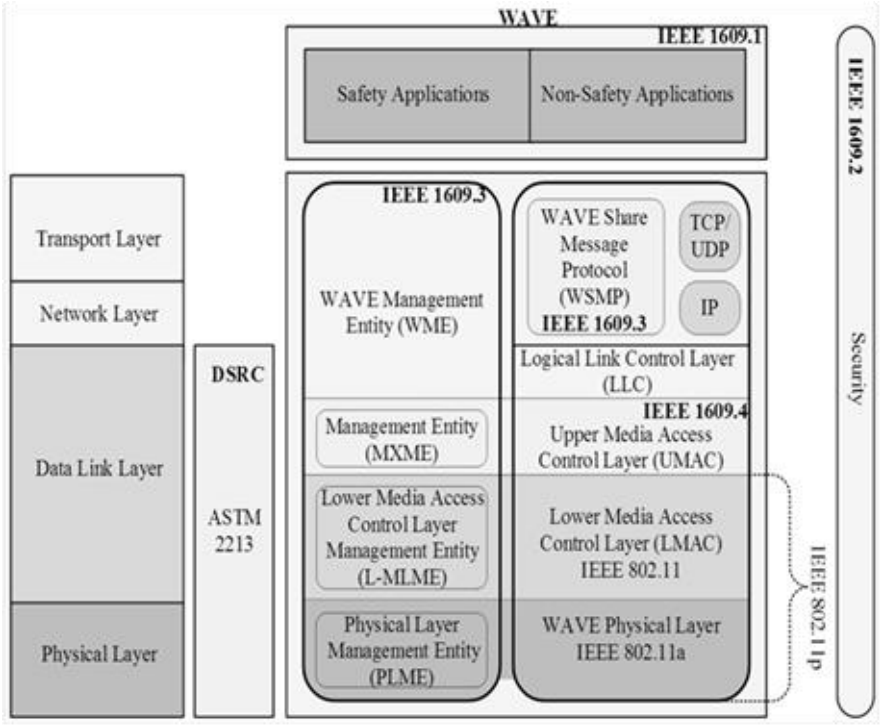


Рис.2 – Модель беспроводного доступа в автомобильном окружении WAVE

Благодаря высокой подвижности транспортных узлов и соответственно динамической топологии формируемой инфокоммуникационной сети, модель мобильности и предсказание положения узлов играют важную роль в проектировании сетевых протоколов. А принимая во внимание, что транспортные узлы обычно ограничены заранее построенными автомагистралями, дорогами и улицами, и соответственно, учитывая скорость и карту улиц, можно предсказать будущее положение транспортных средств. Вышеперечисленные факторы свидетельствуют о необходимости использования при моделировании дорожных карт, схожих по своей структуре с топологией городской среды и применения специализируемых программных средств, формирующих сценарии на основе реалистических моделей мобильности. Для этих целей может быть использован симулятор транспортных потоков SUMO (Simulator of Urban Mobility) [3].

В сетях Vanet стратегия маршрутизации, использующая информацию о географическом положении подвижных узлов, полученную из карт улиц, моделей движения или даже более распространенных навигационных систем на борту транспортных средств, определена как более перспективная парадигма маршрутизации. Большинство позиционно-ориентированных алгоритмов маршрутизации основывают решения на информации о местоположении узлов и перенаправляет пакет к узлу, который географически ближе всего к месту назначения. Кроме этого, сети Vanet сталкиваются с некоторыми проблемами, как безопасность, стабильность и надежность. Повышение производительности сети возможно путем организации кластерной топологии с нечеткими алгоритмами выбора головных узлов и динамическим использованием спектрального диапазона в соответствии с методами когнитивного радио.

Список используемых источников:
ITS EN 302 663 [Электронный ресурс]. – Режим доступа: http://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.02.00_20/en_302663v010200a.pdf
2. IEEE 1609.0-2013 – IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture.
3. Определения и принципы действия SUMO [Электронный ресурс]. – Режим доступа: http://sumo.sourceforge.net/.

ТЕХНОЛОГИЯ VANET. ПРОБЛЕМЫ ВНЕДРЕНИЯ И ПРИМЕНЕНИЯ

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Москалев П.А., Хоменок М.Ю.

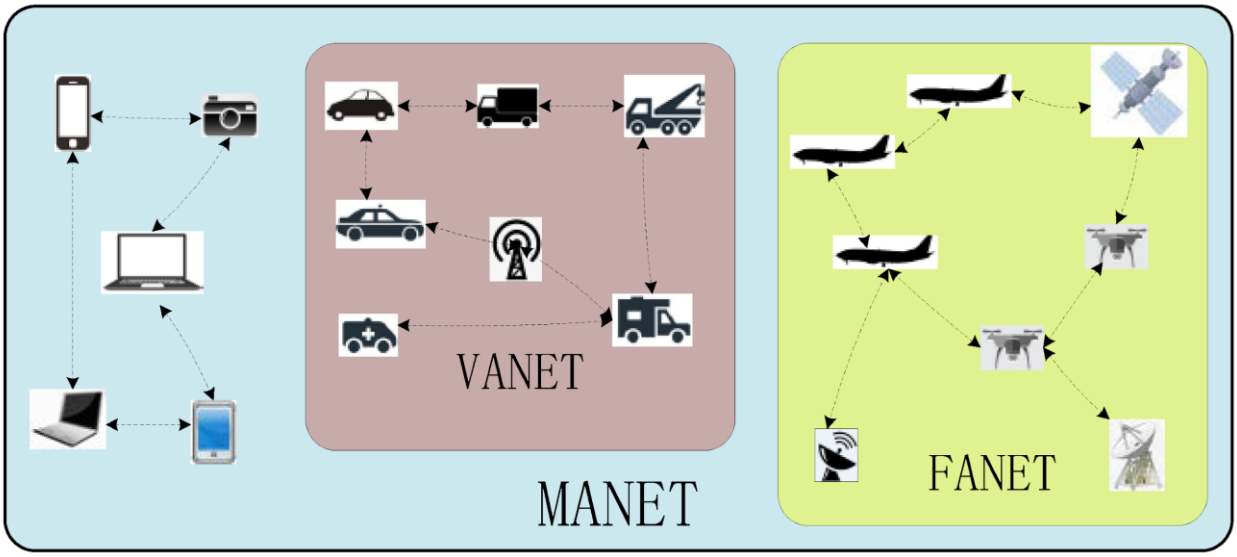
В данной работе рассмотрена технология VANET, ее основные принципы работы, модели применения, проблематика внедрения.

На текущий момент времени технологии продолжают наращивать мощь. Параллельно с развитием мощности компьютерных компонентов, все чаще крупные корпорации задумываются о внедрении в свои технологии элементов искусственного интеллекта, чтобы исключить человеческий фактор.

На текущий момент времени крупными корпорациями автомобильной промышленности, в кооперации с производителями компьютерных компонентов, внедряются системы беспилотного управления, системы – помощники водителю, в дорогие модели автомобилей внедряются камеры с круговым обзором, привязанные к мощным бортовым компьютерам с искусственным интеллектом, основанным на нейронных сетях.

В данной статье рассматривается технология, стоящая у истоков практически всех интеллектуальных систем по управлению автомобилем, организацией движения на дороге и т.д.

Сети VANET – это автомобильные самоорганизующиеся сети. Данная технология уходит корнями в сети MANET, мобильные сети. И хотя изначально технология рассматривалась как копия MANET, с тех пор она стала областью самостоятельных исследований. С 2015 года термин VANET рассматривается как синоним термина – межавтомобильные связи (IVC).



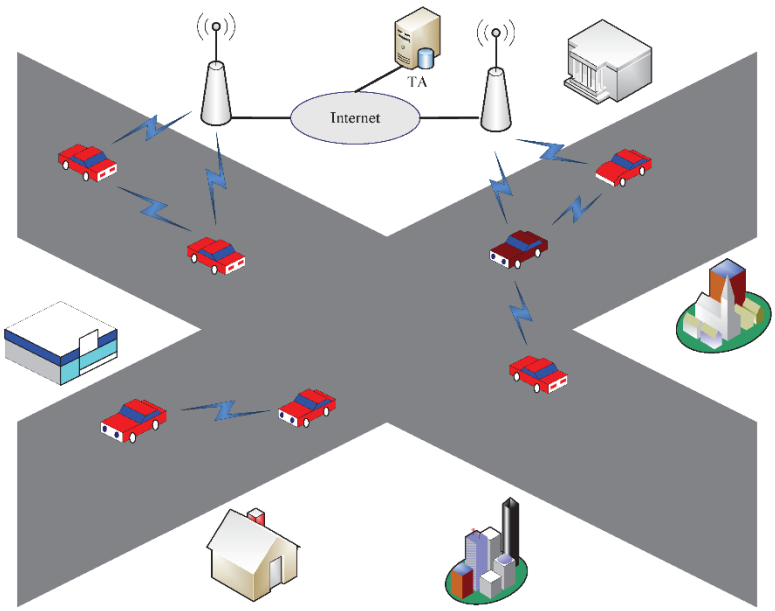
Технология VANET была впервые упомянута и протестирована в 2001 году. Целью данного проекта является создание блоков в транспорте, отслеживающих состояние основных узлов автомобиля (нажатие педалей, включение аварийного сигнала, показания скорости, торможения и т.д.) с целью обмена этими данными с другими автомобилями напрямую или через посредников в лице других автомобилей. Получив данную информацию, блоки в других автомобилях могли оповестить водителя об изменении дорожной обстановки (резкое торможение спереди, приближение транспорта в боковой проекции), и, при необходимости, воздействие на органы управления автомобилем для предотвращения аварийной ситуации.

Основным пунктом данной технологии является то, что выстраиваемая сеть – необслуживаемая и самоорганизовывающаяся. То-есть, она не требует участия человека для своего функционирования, а добавление и удаление новых участников сети происходит автоматически.

Основными сложностями данной технологии являются работа на высоких скоростях и в условиях тяжелого прохождения сигнала. Вопрос быстродействия вызван тем, что на скоростях в 100 и более километров в час при встречном движении сигнал сильно искажается, часть информации может теряться. Для увеличения надежности увеличить сложность обработки

сигнала не представляется возможным. Приведем пример. На скорости в 100 километров в час автомобиль преодолевает примерно 30 метров в секунду. Соответственно при встречном движении скорость сближения автомобилей – 60 метров в секунду. Дальность действия обычного wi-fi роутера – приблизительно 150 метров. При условии, что соединение установилось моментально, чего, разумеется, не может быть, водителю для корректировки остается 2.5 секунды. Добавляем скорость установки соединения, скорость реакции водителя, инерционность автомобиля, шумы от рельефа и метеорологических условий и можно получить цифру намного превышающую 2.5 секунды.

С целью борьбы с данной проблемой, в технологии VANET используется стек протоколов IEEE 802.11p WLAN с частотой работы в районе 5.9 GHz. Данная частота не столь широко используется, соответственно проще выделить сигнал. Дальность действия сигнала больше, чем у сигнала с частотой 2.4 GHz.



Помимо этого, технология VANET предусматривает установку в критичных зонах (перекрестки, развязки, мосты и туннели) установку стационарных узлов, которые связываются с окружающими автомобилями, помогают «проникнуть сигналу за угол». Это приводит к удорожанию внедрения технологии в жизнь.

Помимо этого мобильные операторы и интернет-операторы многих стран оказывают влияние на внедрение данной технологии. С увеличением количества пользователей, приходится расширять спектр используемых частот, а спектр, используемый сетями VANET, является «лакомым куском» для мобильной связи. Часть стран под давлением мобильных операторов вынуждена урезать зарезервированный спектр частот для VANET, что является вопросом конфликта коммерции и безопасности.

Список использованных источников:
1. https://lektsii.org/11-50755.html - определение и принципы действия VANET
2. https://www.sciencedirect.com/topics/computer-science/vehicular-ad-hoc-network - проблематика внедрения и применения

СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ СО ВСТРОЕННОЙ ВИДЕОАНАЛИТТИКОЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Наливайко С.И.

Вишняков В.А. – д.т.н., профессор

Современные системы видео аналитики работают с видеопотоком в реальном времени или из архива. Для детектирования движения, распознавания объектов, создания трека движения необходимо создать фон, с помощью которого можно определить инварианты и меняющиеся пиксели в кадрах. После того, как разностный кадр сформирован, на нем видны белые объекты на черном фоне[1]. Для соотнесения одного объекта между собой на разных кадрах возможно использование различных характеристик, хранящихся в метаданных текущего и предыдущего фреймов. При этом самой важной характеристикой является таймстамп кадра, с помощью которого можно формировать цикл. Возможно возникновение ситуации, когда один объект перекрывает другой, но благодаря трекингу движения и истории этих движений, можно разделить эти объекты и воспринимать их как разные. Важным моментом является попарное сравнение одновременных фреймов с камер, для дальнейшего сшивания их панораму и построению на основе этих цилиндрических кадров видеоанализа потока изображений. Происходит определение инвариантных характеристик соседних изображений. Это достигается с помощью выявления особых точек и их дескрипторов. Особая точка m – точка, которая является изображением окрестности, которой o(m) можно отличить от окрестности любой другой точки изображения o(n) в некоторой другой окрестности особой точки o_2(m) [1].

Для обнаружения особых точек есть несколько алгоритмов, обратим внимание на два из них:

- Speeded Up Robust Features (SURF)
- Scale Invariant Feature Transform (SIFT)

Алгоритм SIFT позволяет определять особые точки в виде капель, так как они инвариантны ко всем преобразованиям. Структуры такого вида являются самыми сложными, высокоуровневыми среди всех видов форм особых точек, и поэтому обеспечивают устойчивое их обнаружение. Одним недостатком SIFT является его вычислительная сложность, что ограничивает его применение в режиме постобработки [2].

Метод SURF решает две задачи – поиск особых точек изображения и создание их дескрипторов (описательного элемента, инвариантного к изменению масштаба и поворота). Кроме того, сам поиск ключевых точек тоже должен обладать инвариантностью, т.е. повернутый объект сцены должен обладать тем же набором ключевых точек, что и образец. Данный метод ищет особые точки с помощью матрицы Гессе. Детерминант матрицы Гессе (т.н. гессиан) достигает экстремума в точках максимального изменения градиента яркости. Матрица Гессе инвариантна к повороту кадра, но не инвариантен к масштабу. В связи с этим в методе SURF используются разномасштабные фильтры для нахождения гессианов. Для каждой ключевой точки считается градиент и масштаб. Градиент в точке вычисляется с помощью фильтров Хаара. Размер фильтра берется равным 4s (где s – масштаб особой точки), а черные области имеют значение «-1», а белые «+1».

Итоговая последовательность всегда обладает ложными соответствиями. Для удаления ложных соответствий применяется метод согласования случайных выборок RANSAC (англ. Random Sample Consensus). Метод RANSAC - вероятностный метод, в котором определяется минимальная погрешность между парами точек, после чего вычисляются коэффициенты матрицы перспективного преобразования H размерности 3x3 (матрица гомографии) методом прямого линейного преобразования DLT (англ. Direct Linear Transformation). Решается система линейных алгебраических уравнений, в результате определяются 8 коэффициентов (параметров DLT), показывающих связь между системами координат плоскостей двух изображений [2].

Разрабатываемая информационная система будет основываться на технологии «клиент-сервер». В виду задачи кроссплатформенности приложения наше приложение будет web-приложением. В виду того, что нами была выбрана архитектура «клиент-сервер» и web-приложение, серверная часть будет написана на языке Java. Вторым языком программирования, позволяющим разрабатывать web-приложения на стороне сервера, был выбран Python.

Список использованных источников:

1. Обработка и анализ изображений в задачах машинного зрения / Ю. В. Визильтер, С. Ю. Желтов, А. В. Бондаренко и др. М.: Физматкнига, 2010 - 672с

2. Herbert Bay, Tinne Tuytelaars, Luc Van Gool, "SURF: Speeded Up Robust Features". Proceedings of the ninth European Conference on Computer Vision, pp. 404 – 417, 2006..

МАСКИРОВАНИЕ ИЗОБРАЖЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Нарейко Д.А.
Шевчук О.Г. – кандидат технических наук

Термин «маскирование» в настоящее время используется в различных областях человеческой деятельности, таких как биология, военное дело, химия, психология, технологии управления базами данных, обработка изображений, цифровая обработка изображений.

В то же время на протяжении последних 8 лет данный термин используется в области защиты от несанкционированного доступа к цифровым изображениям.

Маскирование – процесс преобразования цифровой визуальной информации с малым сроком актуальности к шумоподобному виду с целью защиты от несанкционированного ознакомления. После выполнения маскирования полученный массив информации называется маскированной визуальной информацией или маскированным изображением.

Существующие методы цифрового маскирования изображений можно разделить на два вида:

– криптографическое маскирование или маскирование с использованием криптографических примитивов;

– матричное маскирование.

Криптографическое маскирование – вычислительная процедура прямого преобразования цифровых или аналоговых изображений с применением элементов криптографических методов, разрушающая их до вида, воспринимаемого визуально как шум.

Матричное маскирование – вычислительная процедура преобразования цифровых изображений с использованием матричных операций, разрушающая его до вида, воспринимаемого визуально как шум.

Обычно цифровую обработку применяют к растровым изображениям следующих типов:

– бинарное изображение, элементы которого принимают только два значения {0, 1}. Бинарные изображения в основном получаются в результате обработки полноцветных, палитровых или полутоновых изображений методами бинаризации. При бинаризации изображений используется фиксированный или адаптивный порог бинаризации.

– полутоновое изображение, элементы которого принимают одно из значений интенсивности какого-либо одного цвета. Данный тип изображения является одним из самых распространенных при проведении различных исследований. Самая распространенная глубина цвета на элемент изображения – 8 бит.

– полноцветное изображение, элементы которого непосредственно хранят информацию о яркостях цветовых составляющих.

БЕЗОПАСНАЯ ПОРТАТИВНАЯ ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ С АЛГОРИТМОМ ШИФРОВАНИЯ RABBIT STREAM

Рубинштейн Р. Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Цветков В. Ю. – д. т. н., доцент

В работе рассмотрена безопасная портативная виртуальная частная сеть с алгоритмом шифрования Rabbit Stream и проблемы, связанные с обеспечением ее безопасности и конфиденциальности.

Мобильность сотрудников стала одним из основных требований корпораций в наше время. Сотрудники часто получают командировку в филиалы или клиентские компании, которые находятся внутри или за пределами своей страны. Компания может соединить компьютерную сеть в центральном офисе с ее филиалами, расположенными далеко от Интернета, но она также может предоставить сотрудникам полномочия для доступа к внутренней сети компании. Однако, при передаче информации через Интернет существуют потенциальные уязвимости, такие как: перехват, мониторинг, модификация или изменение информации неуполномоченными сторонами .

Решение, которое можно использовать для преодоления такой уязвимости, заключается в использовании виртуальной частной сети (VPN). Компания предпочитает использовать VPN, а не использовать выделенную линию или выделенный путь провайдера. Помимо большей рентабельности, VPN также обеспечивает функции безопасности, например, шифрование и аутентификация. VPN-туннель сформирован для защиты связи между объектами в системе. OpenVPN является одной из самых популярных платформ VPN с открытым исходным кодом, разработанной Джеймсом Йонаном в 2002 году, и до сих пор продолжает разрабатываться сообществом разработчиков со всего мира.

Что касается платформы поддержки, OpenVPN уже может использоваться на многих платформах, например Операционная система на основе Linux, Debian, BSD, Microsoft Windows, Mac OS X и Solaris 4.

Существует два вида реализации VPN, то есть программная VPN и аппаратная VPN. Программная VPN является наиболее распространенной реализацией VPN. Он может быть установлен поверх операционной системы, поэтому пользователь может осуществлять удаленный доступ через свой ноутбук. Слабость этого типа реализации VPN заключается в том, что он потребляет память или ресурсы ЦП пользовательского ПК во время удаленного доступа. Поэтому производительность пользовательского ПК может быть ниже во время операции удаленного доступа. С другой стороны, в аппаратной VPN, отдельное оборудование используется для работы удаленного доступа. Аппаратная VPN имеет несколько преимуществ. Во-первых, его можно использовать в разных операционных системах ПК пользователя (независимо от платформы). Во-вторых, он более надежен, поскольку построен на отдельном оборудовании от ПК пользователя. В-третьих, у него также есть дополнительные функции, такие как встроенный брандмауэр и интернет-маршрутизация. В последнее время raspberry pi стала решением для ПК с низким энергопотреблением для любых приложений. Некоторые исследования были проведены для разработки аппаратного VPN на Rasberry Pi7,8.

В этом исследовании автор предлагает аппаратный прототип шлюза VPN, который работает на модели OSI уровня 4 (SSL VPN). SSL VPN выбран из-за фактора гибкости или простоты конфигурации, совместимости с трансляцией сетевых адресов (NAT) и отсутствия проблемы с правилами. Аппаратное обеспечение, используемое в предлагаемой системе, - SBC Raspberry Pi 3 Model B + с основными приложениями, которые модифицированы с помощью OpenVPN. Вдобавок к OpenVPN, алгоритм поточных шифров Rabbit реализован как альтернативный вариант шифровальных пакетов TLS. Алгоритм потоковых шифров Rabbit выбран из-за его криптографической стойкости и простых операций 10. Этот алгоритм также был стандартизирован IETF RFC 4503. По результатам тестирования и анализа этот алгоритм доказал свою эффективность в качестве криптографических и устойчивых криптографических аналитических методов.

Исследование состоит из нескольких этапов. Во-первых, мы выявили проблему с традиционным программным обеспечением VPN, как описано во введении. Во-вторых, мы проводим обзор литературы, чтобы найти современное состояние развития технологии VPN, как программного, так и аппаратного решения. В-третьих, мы предъявляем требования к проектированию и планируем разработку аппаратного и программного обеспечения. Наконец, мы выполняем оценку разработанного прототипа. В остальной части этой статьи обсуждается процесс проектирования и оценки прототипа.

Прототип предназначен для поддержки командировочных сотрудников для выполнения удаленного доступа к внутренней сети компании. Мы называем прототип AR-6000. На рисунке 1 показан сценарий использования AR-6000. Из рисунка 1 видно, что в системе зон AR-6000 есть два основных объекта:

• Пользовательская зона путешественника. Это зона, в которой находится деловой путешественник, который выполняет удаленный доступ пользователя. В этой зоне требуются следующие устройства: ПК или ноутбук, AR-6000 и точка доступа WLAN.

• Зона внутренних ресурсов: это местоположение сети внутренних ресурсов, где расположены серверы и компьютеры компании.

Пользователь берет с собой ноутбук AR-6000 во время командировки. AR-6000 действует как VPN-клиент. В случае, если он хочет получить доступ к внутренней сети, AR-6000 сформирует туннель для VPN-сервера. Он применяет SSL VPN для защищенных данных транзакций из внутренних сетей и через них. Затем пользователь может получить удаленный доступ к внутренней сети компании, чтобы продолжить свою работу на сервере. Есть несколько причин, по которым мы превращаем VPN-клиента в отдельное оборудование. Этот прототип предназначен для выполнения следующих требований:

• Прототип должен быть удобным для пользователя, что означает, что он может быть легко использован любым пользователем без необходимости выполнять настройку каждый раз, когда он хочет его использовать.

• Прототип необходим для работы на всех платформах. Это означает, что прототип можно использовать со всеми типами клиентских операционных систем (ОС) с помощью интернет-соединения.

• Если устройство нуждается в реконфигурации, мы можем настроить его, подключившись к устройству через безопасное соединение оболочки (SSH).

• Требуется, чтобы устройство было способно защищать передачу данных от VPN-клиента к VPN-серверу.

Каждый раз, когда пользователь выполняет удаленный доступ к внутренним ресурсам, AR-6000 получает запрос от ПК пользователя через порт Ethernet, который подключен через кроссовер UTP-кабеля, затем пересылает эти запросы на сервер VPN-ретрансляции предполагаемых получателей через интерфейс Wi-Fi. -Fi, интерфейс Wi-Fi, подключенный к точке доступа WLAN. В общем, AR-6000 служит для моста связи между пользователем ПК и внешней сетью, будь то для доступа в Интернет или удаленного доступа к внутренним ресурсам.

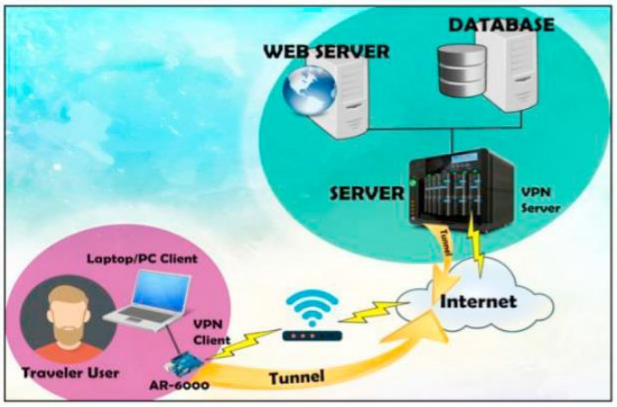


Рисунок 1 Portable VPN usage scenario (AR-6000)

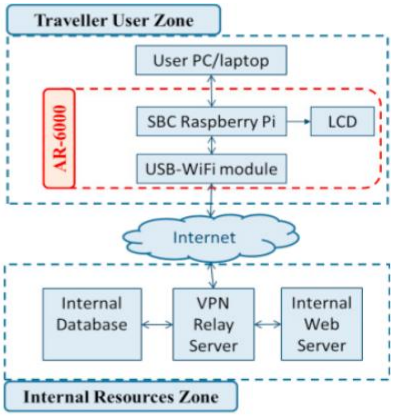


Рисунок 2 Hardware Design of AR-6000

Исходя из требований к дизайну, описанных в предыдущем подразделе, для реализации в пользовательской зоне путешественника и зоне внутренних ресурсов требуется немного оборудования, как показано на рис. 2. В пользовательской зоне путешественника используется пользовательский ПК / ноутбук и AR-6000. AR-6000 состоит из SBC Raspberry Pi 3 Model B + в качестве модуля микроконтроллера, модуля LCD для дисплея и модуля USB Wi-Fi в качестве средства связи. Микроконтроллер организует все функции прототипа AR-6000, например, управление связью с ПК пользователя, маршрутизация, переадресация IP, маскировка IP и т. д. OpenVPN-R устанавливается в качестве основных приложений в микроконтроллере. ЖК-модуль используется для отображения информации, такой как IP-порт Ethernet AR-6000, и для запуска приложения с помощью модуля с сенсорным экраном. Для подключения к Интернету AR-6000 оснащен модулем Wi-Fi в качестве средства связи с ближайшей точкой доступа WLAN. Пользовательский ПК выполняет запрос доступа к серверу ретрансляции VPN через AR-6000. Пользовательский ПК также может настроить AR-6000 через SSH-соединение. С другой стороны,

во внутренней зоне ресурсов есть 3 компонента, то есть сервер ретрансляции VPN, внутренняя база данных и внутренний веб-сервер. Сервер ретрансляции VPN - это компьютер, который используется в качестве цели удаленного доступа пользователя. Он получает и организует запрос удаленного доступа от AR-6000. Open VPN-R также устанавливается на сервере ретрансляции VPN, чтобы создать VPN-туннель к AR-6000 с шифротекстами Rabbit.

Разработка программного обеспечения

В этом разделе рассматривается дизайн программного обеспечения для прототипа переносного VPN. Программный пакет является модификацией OpenVPN. Он называется Open VPN + R. Это программное обеспечение работает на SBC Raspberry Pi Model B + в качестве основных приложений VPN. Принципиальным отличием OpenVPN + R от оригинального OpenVPN является включение шифровальных наборов Rabbit в качестве альтернативного варианта шифровальных наборов TLS для защиты пути или канала данных транзакции. OpenVPN использует OpenSSL для криптографических алгоритмов и предоставления шифровальных пакетов TLS. Поэтому, чтобы добавить шифровальные наборы Rabbit в OpenVPN-R, необходимо реализовать алгоритмы для потоковых шифров Rabbit в OpenSSL и изменить OpenVPN, чтобы они могли распознавать алгоритм потокового шифра, который реализован в OpenSSL Rabbit.

Для осуществления реализации необходимо разработать новые наборы шифров TLS, которые представляют собой комбинацию нескольких криптографических алгоритмов с алгоритмом шифрования потока Кролика в качестве алгоритма шифрования данных (алгоритм массового шифрования). Комбинация криптографических алгоритмов состоит из алгоритмов аутентификации сервера, алгоритмов обмена ключами, алгоритмов шифрования данных и алгоритмов дайджеста сообщений. Новые наборы шифров TLS, сделанные в этом исследовании, относятся к стандарту протокола TLSv1.2 (RFC 5246), как определено в таблице 2.

Ciphersuites Rabbit	Authentication	Key Change	Encryption	Message Digest
TLS_RSA_WITH_RABBIT_SHA	RSA	RSA	RABBIT	SHA
TLS_DHE_DSS_WITH_RABBIT_SHA	DSS	DSS	RABBIT	SHA
TLS_DHE_RSA_WITH_RABBIT_SHA	RSA	RSA	RABBIT	SHA

Таблица 2 Protocol Ciphersuite Rabbit in Open VPN-R

В этом исследовании используется OpenSSL версии 1.0.2h, которая, как утверждается, успешно закрыла пробел в безопасности. В общем случае реализация модификации исходного кода будет осуществляться как в библиотеках OpenSSL, так и в библиотеке криптографии и в библиотеке SSL. Добавления в библиотеку криптографии необходимы, потому что в этой библиотеке хранятся все криптографические функции, включая алгоритм шифрования потока Кролика, который будет реализован. Что касается библиотеки SSL, то основное внимание уделялось добавлению новых наборов шифров, в результате чего была реализована реализация SSL, поддерживающая использование алгоритма потокового шифра Rabbit. Его также необходимо изменить в некоторых скриптах компиляции, чтобы исходный код реализованного алгоритма потокового шифра Rabbit можно было интегрировать с OpenSSL. Результатом этого этапа реализации является версия OpenSSL 1.0.2h, которая загрузила алгоритм потокового шифра Rabbit в качестве одного из альтернативных вариантов алгоритма шифрования, как для кодирования на наборах TLS, так и для ручного кодирования через консольное приложение OpenSSL.

После завершения реализации алгоритма потокового шифра Rabbit, следующий будет изменен и перекомпилирован на OpenVPN для распознавания алгоритма потокового шифра Rabbit, реализованного в OpenSSL. OpenVPN, используемый в этом исследовании, является версией OpenVPN 2.3.10. Как только изменения в OpenVPN завершены, результатом является версия 2.3.10 OpenVPN, которая уже может распознавать алгоритм шифрования потока Кролика. Версия OpenVPN называется OpenVPN-R, которая будет использоваться в качестве основного приложения устройств AR-6000.

Список использованных источников:0

1.Choffnes D. A case for personal virtual networks. In: Proceedings of the 15th ACM Workshop on Hot Topics in Networks. 2016. p. 8– 14.

2.Alshalan A, Pisharody S, Huang D. A survey of mobile VPN technologies. IEEE Commun Surv Tutorials. 2016;18(2):1177–96.

3.Matotek D, Turnbull J, Lieverdink P. Networking with VPNs. In: Pro Linux System Administration. Springer; 2017. p. 701–31.

НОВЫЙ ПОДХОД К ПОВЫШЕНИЮ БЕЗОПАСНОСТИ MPLS VPN ПУТЕМ ПРИНЯТИЯ ПРОГРАММНО-ОПРЕДЕЛЯЕМОЙ СЕТЕВОЙ ПАРАДИГМЫ

Рубинштейн Р. Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Цветков В. Ю. – д. т. н., доцент

В работе рассмотрен новый подход к повышению безопасности MPLS VPN путем принятия программно-определяемой сетевой парадигмы

Безопасность сетевых инфраструктур является одной из утомительных задач в современных сетях. Действительно, в наши дни требуемая безопасность должна характеризовать динамизм и способность адаптироваться к контексту бирж, другими словами, безопасность не должна влиять на производительность сети. Чтобы удовлетворить эту потребность, можно использовать автоматизацию сети через контроллер программно-определяемой сети (SDN). SDN - новая парадигма, позволяющая через контроллер управлять всей архитектурой сети. В этой статье мы предлагаем новое решение для динамической генерации политик безопасности между различными сайтами MPLS VPN путем принятия подхода SDN. Безопасность является одной из основных задач бизнеса, поскольку безопасность - это не только конфиденциальность, целостность или аутентификация, но и высокая доступность. Высокая доступность зависит от нескольких факторов, а именно от используемого оборудования, стратегий и планов, предоставляемых компанией в случае неисправности системы. Иногда компании могут потребоваться четыре основных принципа безопасности, поэтому для поиска компромисса и решения, гарантирующего их, требуется много внимания. Например, протоколы шифрования или политики безопасности трафика в целом могут влиять на производительность оборудования и, таким образом, ставить под угрозу доступность ресурсов.

Многопротокольная коммутация по меткам «MPLS» рассматривается как основной протокол, развернутый на уровне ядра сети оператора. MPLS был успешным с появлением новых связанных сервисов, прежде всего сервиса виртуальной частной сети (VPN) . MPLS VPN позволяет получить безопасное соединение с меньшими затратами. Поэтому для создания клиентских VPN необходимо изолировать потоки каждого клиента.

Это правда, что MPLS VPN обеспечивает высокий уровень безопасности по сравнению с традиционными VPN, потому что трафик проходит через частную сеть оператора, но некоторые клиенты предпочитают добавлять уровень шифрования через протокол IPsec . IPsec также опирается на два протокола: 1) аббревиатуру заголовка аутентификации для AH, гарантирующую аутентификацию, целостность и защиту от повторного воспроизведения данных, 2) полезную нагрузку инкапсуляции "ESP", обеспечивающую большую конфиденциальность.

С появлением облака видим дополнительный шаг в автоматизации процессов с помощью Software Defined Network (SDN). Это значительно упрощает автоматизированные операции в стандартных и воспроизводимых средах. Благодаря этому новому режиму работы этапы тестирования и развертывания сокращены, что существенно экономит время и деньги. SDN позволяет по принципу оркестровки управлять сетевыми ресурсами компании из центральной точки, называемой контроллером. Парадигма SDN может быть принята для реализации новых правил для улучшения политик безопасности защищенных IPsec туннелей MPLS VPN с целью удовлетворения потребностей компании, особенно с точки зрения безопасности, целостности, аутентификации и особенно доступности.

Подход состоит из трех этапов: измерение производительности сети (приложения и оборудование), расчет соответствующей политики IPsec и развертывание этой политики на маршрутизаторах и устройствах. Эти шаги вращаются вокруг четырех элементов: доступность, конфиденциальность, целостность и аутентификация.

Список использованных источников:0

1. Bensalah, F., & El Kamoun, N. (2019). Novel software-defined network approach of flexible network adaptive for VPN MPLS traffic engineering. International Journal of Advanced Computer Science and Applications, 10(4), 280-284.

2. Bahnasse, A., Louhab, F. E., Ait Oulahyane, H., Talea, M., & Bakali, A. (2018). Novel SDN architecture for smart MPLS traffic engineering-DiffServ aware management. Future Generation Computer Systems, 87, 115-126.

МЕТОДИКА РАЗВЕРТЫВАНИЯ И КОНФИГУРИРОВАНИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сакович Д. А.

Бобов М. Н. – д-р. техн. наук, профессор

Межсетевой экран представляет собой специальное решение для обеспечения безопасности сети. Его функция заключается в постоянном мониторинге входящего и исходящего трафика и его фильтрации на основании установленных правил. Благодаря этому обеспечивается создание защитной стены между внутренней и внешней сетью.

При выборе межсетевого экрана для развертывания необходимо учесть следующие моменты:

- Необходимая категория межсетевых экранов – оборудование, программное обеспечение, программно-аппаратных комплекс.
- Особенности конфигурации сети, которые могут повлиять на выбор межсетевого экрана, например, необходимость поддержки заданного количества пользовательских сессий без ущерба производительности, возможность организации подсетей и другие.
- Используемые механизмы сетевой безопасности - возможности межсетевого экрана и способность решать конкретные задачи.
- Пропускная способность и ее параметры при разных режимах работы.
- Количество портов LAN, WAN, DMZ.
- Особенности конструктивного исполнения (для оборудования).
- Затраты на покупку, эксплуатацию, обслуживание.

Различают следующие типы межсетевых экранов[1][2]:

- Управляемые коммутаторы.
- Пакетные фильтры.
- Шлюзы сеансового уровня.
- Посредники прикладного уровня.
- Инспекторы состояния.
- Управляемые коммутаторы

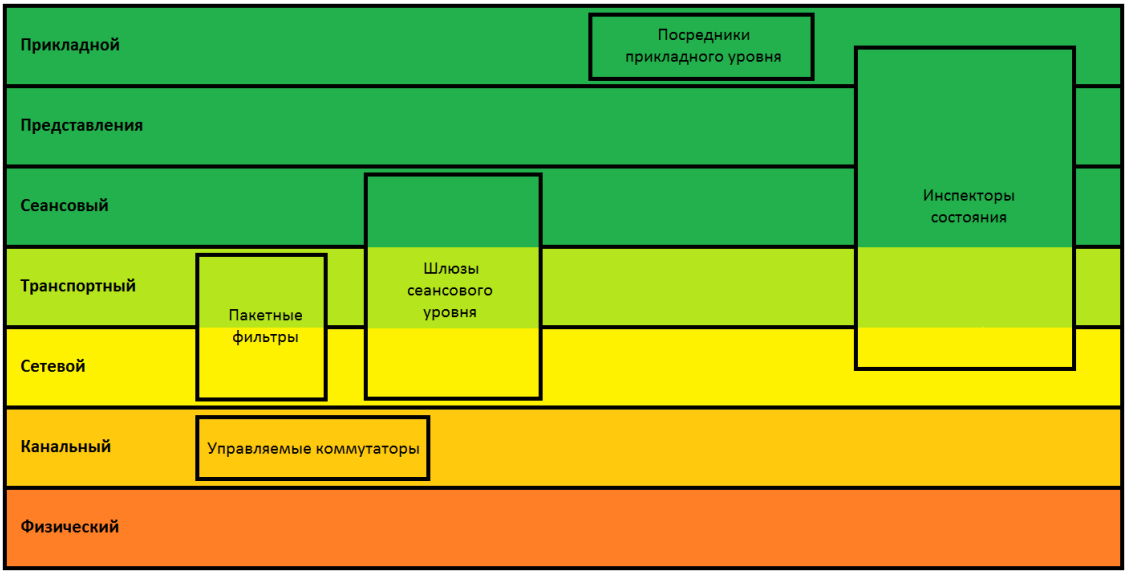


Рисунок 1 – Схематическое изображение классификации межсетевых экранов на основе сетевой модели OSI

При реализации политики безопасности в рамках корпоративной сети, основу которых составляют управляемые коммутаторы, они могут быть мощным и достаточно дешёвым решением. Взаимодействуя только с протоколами канального уровня, такие межсетевые экраны фильтруют трафик с очень высокой скоростью. Основным недостатком такого решения является невозможность анализа протоколов более высоких уровней[2].

Пакетные фильтры функционируют на сетевом уровне и контролируют прохождение трафика на основе информации, содержащейся в заголовке пакетов. Многие межсетевые экраны данного типа могут оперировать заголовками протоколов и более высокого, транспортного, уровня (например, TCP или UDP). Пакетные фильтры одними из первых появились на рынке межсетевых экранов и по сей день остаются самым распространённым их типом. Данная технология реализована в подавляющем большинстве маршрутизаторов и даже в некоторых коммутаторах[3].

Межсетевой экран сеансового уровня исключает прямое взаимодействие внешних хостов с узлом, расположенным в локальной сети, выступая в качестве посредника (англ. proxy), который реагирует на все входящие пакеты и проверяет их допустимость на основании текущей фазы соединения. Шлюз сеансового уровня гарантирует, что ни один сетевой пакет не будет пропущен, если он не принадлежит ранее установленному соединению [1].

Так как межсетевой экран данного типа исключает прямое взаимодействие между двумя узлами, шлюз сеансового уровня является единственным связующим элементом между внешней сетью и внутренними ресурсами. Это создаёт видимость того, что на все запросы из внешней сети отвечает шлюз, и делает практически невозможным определение топологии защищаемой сети. Кроме того, так как контакт между узлами устанавливается только при условии его допустимости, шлюз сеансового уровня предотвращает возможность реализации DoS-атаки, присущей пакетным фильтрам.

Посредники прикладного уровня

Межсетевые экраны прикладного уровня, к которым, в частности, относится файрвол веб-приложений, как и шлюзы сеансового уровня, исключают прямое взаимодействие двух узлов. Однако, функционируя на прикладном уровне, они способны «понимать» контекст передаваемого трафика. Межсетевые экраны, реализующие эту технологию, содержат несколько приложений-посредников, каждое из которых обслуживает свой прикладной протокол. Такой межсетевой экран способен выявлять в передаваемых сообщениях и блокировать несуществующие или нежелательные последовательности команд, что зачастую означает DoS-атаку, либо запрещать использование некоторых команд (например, FTP PUT, которая даёт возможность пользователю записывать информацию на FTP сервер).

Посредники прикладного уровня способны выполнять аутентификацию пользователя, а также проверять, что SSL-сертификаты подписаны конкретным центром. Межсетевые экраны прикладного уровня доступны для многих протоколов, включая HTTP, FTP, почтовые (SMTP, POP, IMAP), Telnet и другие[2].

Инспекторы состояния

Каждый из вышеперечисленных типов межсетевых экранов используется для защиты корпоративных сетей и обладает рядом преимуществ. Однако, куда эффективней было бы собрать все эти преимущества в одном устройстве и получить межсетевой экран, осуществляющий фильтрацию трафика с сетевого по прикладной уровень. Данная идея была реализована в инспекторах состояний, совмещающих в себе высокую производительность и защищённость.

Осуществляя фильтрацию трафика по принципу шлюза сеансового уровня, данный класс межсетевых экранов не вмешивается в процесс установления соединения между узлами. Поэтому производительность инспектора состояний заметно выше, чем у посредника прикладного уровня и шлюза сеансового уровня, и сравнима с производительностью пакетных фильтров [1].

Межсетевые экраны не являются панацеей при борьбе с атаками злоумышленников. Они не могут предотвратить атаки внутри локальной сети, но вместе с другими средствами защиты играют исключительно важную роль для защиты сетей от вторжения извне. Понимание технологии работы межсетевых экранов позволяет не только сделать правильный выбор при покупке системы защиты, но и корректно настроить межсетевой экран.

Список использованных источников:

1. Лебедь С. В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. — МГТУ им. Н. Э. Баумана, 2002. — 306 с.

2. Чепмен-мл. Д. В., Фокс Э. Брандмауэры Cisco Secure PIX = Cisco® Secure PIX® Firewalls. — Вильямс, 2003

3. Фаронов А. Е. Основы информационной безопасности при работе на компьютере. — ИНТУИТ, 2016. — 155 с.

РАЗРАБОТКА ЗАЩИТЫ КОМПЬЮТЕРНОЙ СЕТИ ОТ УГРОЗ ИЗ ВНЕШНЕЙ СРЕДЫ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сорокин С.А., Гурин И.А.

Вишняков В.А – д.т.н., профессор

Согласно отчету лаборатории Касперского III квартал 2015 года характеризовался значительно возросшим количеством атак хакеров, направленных на отказ работы информационных систем. Причём география подобных сетевых угроз достаточно широка – DDoS-атакам подвергались цели в 79 странах мира. При этом 91 % атакованных ресурсов приходится на 10 стран мира. Лидерами по количеству DDoS-атак являются США, Китай и Республика Корея. Кроме широкого географического распространения, следует отметить огромное количество аппаратных и финансовых ресурсов, потраченных на некоторые сетевые атаки. В 2015 году самая продолжительная DDoS-атака продолжалась 13,3 дней [6][1].

Наиболее известные нарушения информационной безопасности компьютерных сетей – сбои, отказы, стихийные бедствия, побочные влияния и ошибки. Смысл этих явлений (кроме стихийных бедствий) выражается следующим образом [7, 8]:

• отказ – сбой в работе какого-либо элемента системы, приводящий к невозможности выполнения им основных своих функций;

• сбой – временное нарушение в работе какоголибо элемента системы, вследствие чего он не может выполнять свои функции;

• ошибка – неправильное (единичное или периодичное) выполнение элементом одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния;

• побочное влияние – негативное воздействие на отдельные элементы системы или на нее в целом, оказываемое какими-либо явлениями, происходящими во внешней среде или внутри системы.

Самыми неуязвимыми для вирусов и удалённых сетевых атак считались операционные системы Apple, но в последнее время, как показывает статистика, они всё чаще подвергаются атакам вредоносных программ. За первые девять месяцев 2015 года подобных атак на системы Apple было в семь раз больше, чем за весь предыдущий год, а пик заражений пришелся на первый квартал 2015 года. Например, в марте было предпринято более 65 тыс. атак на компьютеры фирмы Apple [9].

Команда экстренного реагирования на киберугрозы промышленных систем управления – ICSCERT, выпустила в США доклад «Incident response/vulnerability coordination in 2014», в котором была приведена статистика инцидентов информационной безопасности в автоматизированных системах управления технологическими процессами (АСУ ТП) и критически важных объектах. В докладе приведен обзор состояния информационной безопасности в АСУ ТП и критически важных объектах. В России пока такая статистика не приводится, хотя в ближайшем будущем планируется создать собственный CERT [11][3].

По итогам 2014 года ICS-CERT получила от владельцев критически важных объектов и отраслевых партнеров информацию о более 200 нарушениях информационной безопасности. Лидером по количеству выявленных нарушений является энергетический сектор. При этом сотрудничество энергетического сектора и CERT дает возможность эффективно реагировать на подобные нарушения [12]. Следует упомянуть, в 2014 году были сообщения об нарушениях в критически важных секторах промышленности, включая АСУ ТП производителей оборудования. Поставщики промышленного оборудования АСУ ТП – одна из главных целей для экономической разведки и шпионажа [12][2].

Около 55 % обнаруженных нарушений приходится на направленные атаки и действия квалифицированных злоумышленников. К другим нарушителям относят: хактивистов, преступные элементы, внутренних нарушителей. В большинстве случаев злоумышленники остаются неизвестными [13]. Распределение нарушений информационной безопасности по секторам промышленности представлено на рисунке 1 [11]. Размер негативного воздействия нарушений (инцидентов) и количество методов воздействия с целью получения несанкционированного доступа к инфраструктуре бизнес-систем и АСУ ТП достаточно широк. На рисунке 2 приведен пример некоторых из них [14].

Распределение нарушений в критически важных объектах и АСУ ТП по векторам атак представлено на рисунке 3 [11].

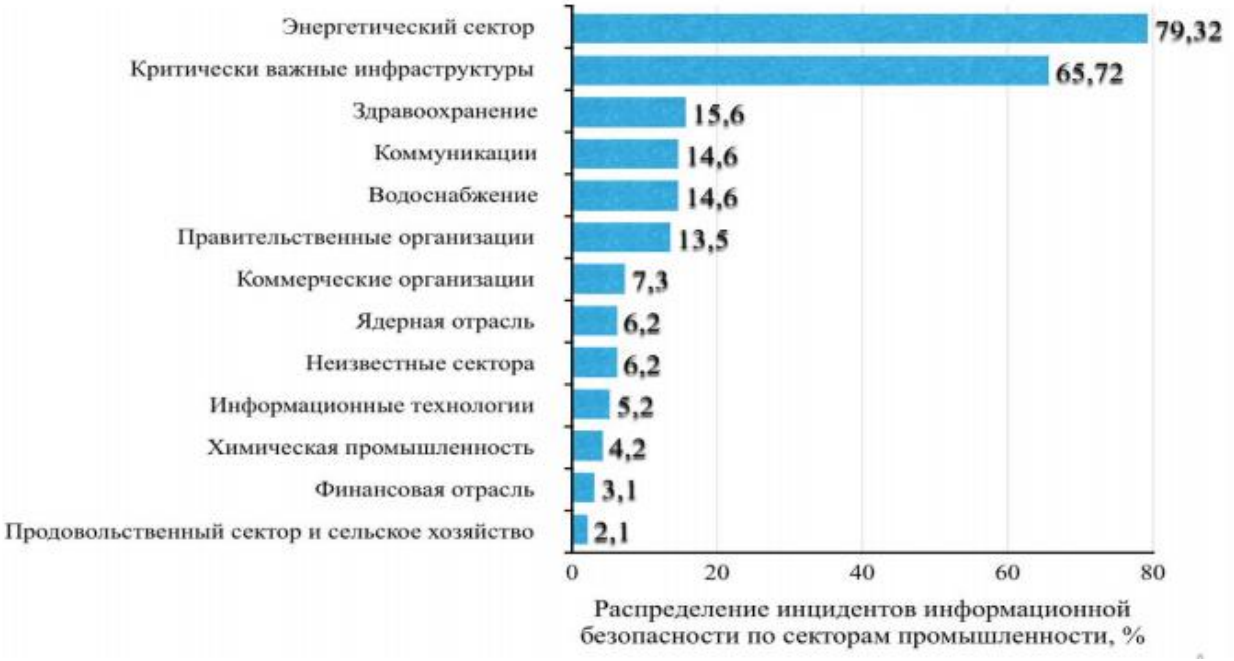


Рисунок 1 – Распределение нарушений информационной безопасности по секторам промышленности

Несанкционированный доступ и эксплуатация внешнего web client-side АСУ ТП или SCADA	Перемещение между сегментами сети	Эксплуатация уязвимостей нулевого дня в контролирующих устройствах и программном обеспечении
Распространение инфекций в беспроводных сетях систем управления	**Инциденты**	SQL инъекции через эксплуатацию уязвимостей веб-приложений
Сканирование и зондирование сети	Атаки на веб-сайты (watering hole)	Таргетированные атаки посредством социальной инженерии в электронной почте

Рисунок 2 – Примеры негативного воздействия нарушений (инцидентов)

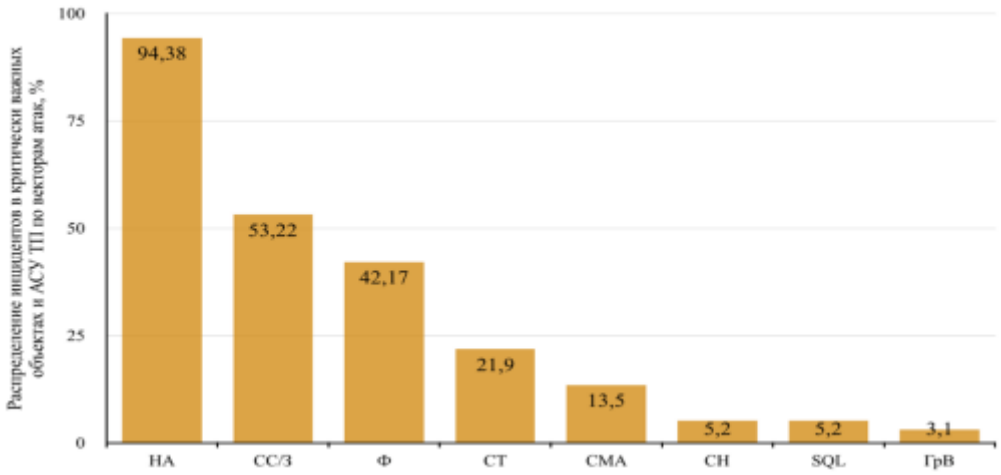


Рисунок 3 – Нарушения в критически важных объектах и АСУ ТП по векторам атак НА – неизвестные атаки, СС/З – сканирование сети/зондирование, Ф – фишинг по e-mail, СТ – смешанные типы, СМА – слабые механические аутентификации, СН – съемные носители, SQL–SQL – инъекции, ГрВ – «грубые» вторжения

На первый взгляд достаточно простыми и наименее финансово-затратными выглядят административные меры обеспечения информационной безопасности сетей предприятия. Основная цель принимаемых мер на административном уровне – разработка программы работ в области улучшения доступности информационных услуг и обеспечение их выполнения, выделяя необходимые ресурсы и контролируя фактическое положение дел [15].

На первом этапе по разработке программы анализируют угрозы и риски.

Средства обеспечения информационной безопасности в зависимости от их реализации разделяют на классы методов (рис. 4) [17].

Типы защиты сети можно разбить на четыре основные категории (рис. 5) [17, 18].

1. Физическая безопасность. Любой компьютер, будь то рабочая станция, сетевой сервер, общественный терминал в уличном киоске или ноутбук, нуждается в обеспечении физической защитой. 2

2.. Безопасность пользователей имеет следующие аспекты:

• возможность предоставления пользователям доступа к информационным ресурсам в соответствии с их потребностями;

• необходимость не предоставлять (а в некоторых случаях скрывать) от пользователей ресурсов ту информацию, которая не требуется им для работы. К такой информации относится важная для компании информация и персональные данные. Контроль доступом заключается во взаимном опознании пользователя и системы и определении степени допустимости использования того или иного ресурса конкретным пользователем в соответствии с его запросом.

3. Защита файлов также имеет некоторые аспекта:

• управление доступом к файлам;

• защита целостности файла. Преступник намеренно вошедший в систему может уничтожить, удалить или изменить информацию в файлах. Поэтому рекомендуется ввести некоторые ограничения на обработку файлов, являющихся носителями важной информации.

4. Защита от несанкционированного входа реализуется с помощью процедур регистрации обращений, идентификации и аутентификации [4][21].

Идентификация и аутентификация могут быть сделаны в ходе работы неоднократно для исключения возможности доступа к системе злоумышленников, выдающих себя за истинного пользователя.

Централизованное администрирование подразумевает, что один человек, группа или отдел осуществляют административное управление всей корпоративной сетью, ресурсами и пользователями. Главным и достаточно серьезным недостатком централизованной схемы является ее недостаточная масштабируемость и отсутствие отказоустойчивости. От производительности центрального компьютера зависит число пользователей, работающих с приложениями, и выход из строя центрального компьютера приведет к нарушению работы всех пользователей [19, 20]. Данную модель хорошо применять в небольших и средних организациях, а для для крупных или территориально распределенных предприятий она может быть неэффективной. Однако, учитывая вопросы безопасности, централизованное администрирование является лучшим. Оно гарантирует единство системной политики и процедур для всей организации [5].

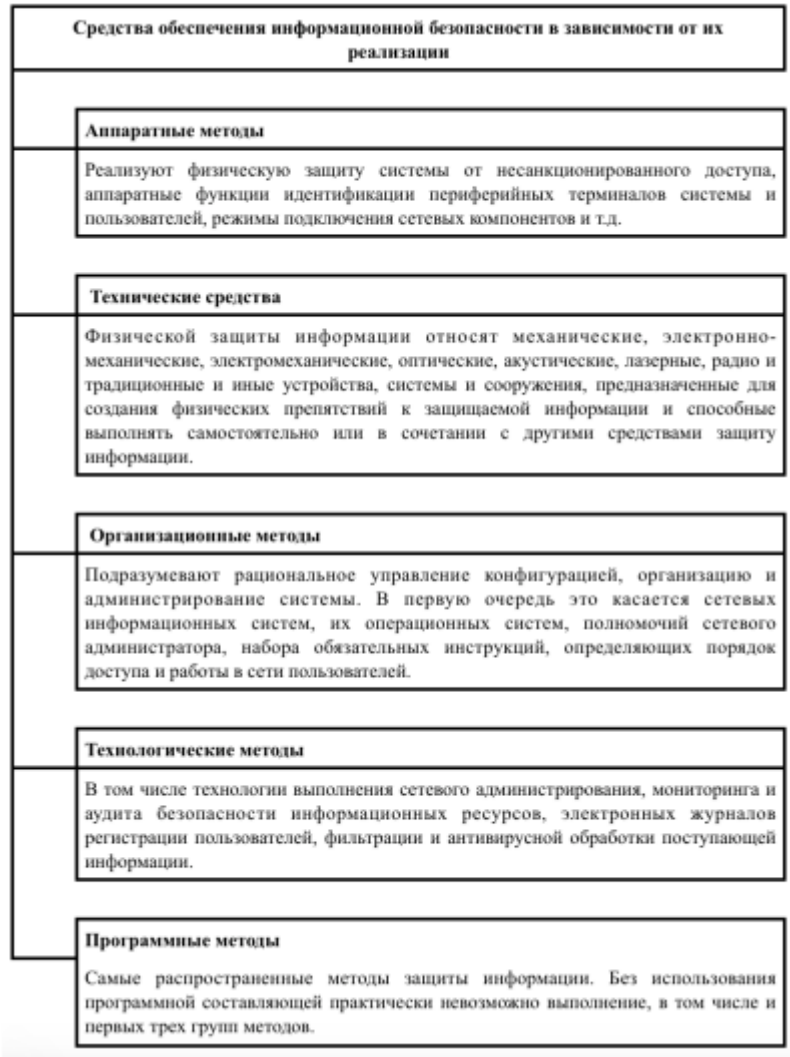


Рисунок 4 – Средства обеспечения информационной безопасности в зависимости от их реализации

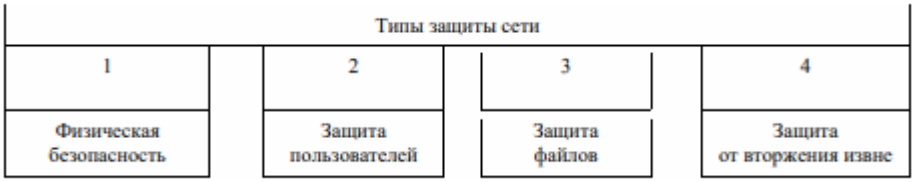


Рисунок 5 – Типы защиты сети

Распределенное администрирование сети подразумевает управление, осуществляющееся на уровне отдела или рабочей группы. Хотя администрирование на этом уровне имеет возможность оперативно реагировать на потребности пользователей, зачастую это достигается за счет сетевой безопасности. Если на предприятии несколько администраторов, политика администрирования в различных рабочих группах будет отличаться. Чем больше число групп, тем больше доверительных отношений, в которых они нуждаются, что повышает вероятность проникновения злоумышленников в систему с целью получения секретной информации, используя доверительные отношения [19, 20].

Администрирование на уровне операционных систем включает в себя средства безопасности существенно различающиеся в зависимости от используемых операционных систем. Например, имеется администратор серверов Windows NT, серверов Novell Net Warel и серверов Unix-систем, каждый из них гарантирует безопасность своей сети. Тем не менее необходим специалист, который будет урегулировать разногласия администраторов в случае возникновения проблем [19, 20].

Смешанная модель администрирования сочетает в себе распределенную и централизованную модели. Центральный администратор (или группа) обеспечивает проведение политики безопасности в масштабах всего предприятия, а администраторы на уровне отделов или рабочих групп выполняют повседневную работу. Это обычно требует больше затрат для содержания штата сотрудников, поэтому использование смешанной модели управления чаще применяется крупными предприятиями [19, 20].

Политика безопасности должна применяться в рамках всей организации.

Несмотря на соответствие самым строгим требованиям безопасности, если система некорректно спроектирована и плохо управляется, то возможна неэффективная защита и сложность использования системы по прямому назначению. Необходимо учитывать, что повышение уровня безопасности системы требует больше времени и административных усилий, чтобы управлять ими.

При построении системы защиты целесообразно придерживаться следующих принципов:

- актуальность, чтобы обезопасить себя от реальных атак, а не от фантастических или архаичных;

- обоснованность расходов, поскольку 100 % защита нереальна, необходимо найти точку, в которой дальнейшие расходы на повышение безопасности будут превышать стоимость информации, которую злоумышленники могут украсть [21].

Список использованных источников:

1. Варфоломеев А. А. Основы информационной безопасности: Учеб. пособие. М. : РУДН, 2008. 412 с.

2. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. М. : НПЦ «Аналитика», 2008. 436 с.

3. Alan G. Konheim – Computer security and cryptography. Изд-во : John Wiley & Sons, Inc., 2007. 542 с.

4. Артемьева Ю. В. Маркетинговая безопасность? Принцип работы // Маркетинг в России и за рубежом. 2011. № 6. С. 32–38.

5. Ломаков Ю. А. Методики оценивания рисков и их программные реализации в компьютерных сетях // Молодой ученый. 2013. № 2. С. 43–46.

6. DDoS-атаки в третьем квартале 2015 года [Электронный ресурс] URL: https://securelist.ru/files/ 2015/11/Q3_DDoS_report_RUS.pdf (дата обращения: 07.01.2016).

7. Абрамов Н. С., Фраленко В. П. Угрозы безопасности вычислительных комплексов: классификация, источники возникновения и методы противодей- ствия // Программные системы: теория и приложения. 2015. № 6:2 (25). С. 63–83.

8. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации: учебное пособие. М. : Центр ЕАОИ, 2012. 311 с.

9. Число вирусных атак на компьютеры Apple выросло в семь раз [Электронный ресурс] URL: http://itbusiness.com.ua (дата обращения: 09.01.2016).

10. Symantec: количество угроз для OS X и iOS продолжает расти раз [Электронный ресурс] URL: http://club-symantec.ru (дата обращения: 09.01.2016).

11. Статистика инцидентов, угроз и уязвимостей информационной безопасности в КВО и АСУ ТП [Электронный ресурс] URL: https: // tosaithe.wordpress.com (дата обращения: 09.01.2016).

12. Отчёт ICS-CERT за июль-август [Электронный ресурс] URL: http://www.securitylab.ru (дата обращения: 09.01.2016).

13. Синещук Ю. И. Основные угрозы и направления обеспечения безопасности единого информационного пространства / [и др.] // Вестн. С.-Петерб. ун-та МВД России, 2013. № 2. С. 150–154.

14. Алаева С. С., Бобков С. П., Ситанов С. В. Администрирование в информационных системах: учеб. пособие / Иван. гос. хим.-технол. ун-т. Иваново, 2010. 52 с.

15. Крат Ю. Г., Шрамкова И. Г. Основы информационнойбезопасности : учеб. пособие. Хабаровск : Изд-во ДВГУПС, 2008. 112 с.

16. Громов Ю. Ю., Иванова О. Г., Мосягина Н. Г., Набатов К. А. Надёжность информационных систем : учебное пособие / Тамбов : Изд-во ГОУ ВПО ТГТУ, 2010. 160 с.

17. Жигулин Г. П. Организационное и правовое обеспечение информационной безопасности. СПб. : СПб НИУИТМО, 2014. 173 с.

18. ЗавгороднийВ. И. Комплексная защита информации в компьютерных системах: учебное пособие. М. : Логос; ПБОЮЛ Н. А. Егоров, 2001. 264 с.

19. Туккель И. Л. Методы и инструменты управления инновационным развитием промышленных предприятий. СПб. : БХВ-Петербург, 2013. 208 с.

20. Кустов Н. Т. Администрирование информационно-вычислительных сетей : учебное пособие. Томск : Томскийгосударственныйуниверситет, 2004. 247 с.

21. Вишняков В.А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения – Минск, 2012. – 274 с.: ил. (С.11-21. Раздел 1. Основные проблемы информационной безопасности).

ПРИМЕНЕНИЕ СЕНСОРНЫХ СЕТЕЙ В СИСТЕМЕ УПРАВЛЕНИЯ МОБИЛЬНЫМИ РОБОТОТЕХНИЧЕСКИМИ КОМПЛЕКСАМИ

Турлай А.П.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Саломатин С.Б. – канд. тех. наук, доцент

Основной проблемой в системах управления роботизированными комплексами в настоящее время остается скорость и достоверность получения информации (команд) объектами управления, получение телеметрических данных оператором при использовании сенсорных измерительных сетей.

В сложных помеховых условиях сенсорные измерительные сети имеют дело со значительными искажениями полезных сигналов. Задача восстановления информации по искаженным сигналам является актуальной и решается разными методами [1-2].

Один из способов восстановлении информации предполагает использования разреженных алгоритмов реконструкции.

В докладе рассматривается модель распределенной сенсорной сети, с измерением коррелированных разреженных сигналов и алгоритмов разреженной аппроксимации. Предполагается, что сеть состоит из нескольких соединенных между собой узлов, и базовые данные, собранные в узлах, коррелированы.

Модель сети. В сети p-й датчик измеряет сигнал $\mathbf{x}_p \in \mathbb{R}^N$ в соответствии со следующим соотношением

$$\mathbf{y}_p = \mathbf{A}_p \mathbf{x}_p + \mathbf{e}_p, \ \forall p \in L,$$

где $\mathbf{y}_p \in \mathbb{R}^M$ - вектор измерения, $\mathbf{A}_p \in \mathbb{R}^{M \times N}$ - матрица измерения, $\mathbf{e}_p \in \mathbb{R}^M$ - шум измерения, а L - глобальный набор, содержащий все узлы в сети. В сети используются измерительные матрицы $\mathbf{A}_p$, которые имеют единичные столбцы с ℓ_2-нормой. В модели $M < N$. $\mathbf{A}_p$ и $\mathbf{e}_p$ независимы как локально, так и по всей сети. Сигнальный вектор $\mathbf{x}_p = [x_p(1), x_p(2), \dots, x_p(N)]$ является T-разреженным, что означает, что у него есть T элементов, которые не равны нулю. Индексы элементов, соответствующие ненулевым значениям, собираются в наборе поддержки T_p, что означает $T_p = \{i : x_p(i) \neq 0\}$ и $|T_p| = \mathrm{T}$. Модель сигнала, предусматривает корреляцию между векторами $\{\mathbf{x}_p\}$.

Для разреженного сигнала $\mathbf{x}_p$ опорный набор T_p следует из конструкции

$$T_p = I_p \cup J_p = I_p \cup J, \qquad \forall p \in L.$$

Частичный набор поддержки $J_p = J$ является объединенным (то есть общим) с наборами поддержки всех разреженных сигналов, что приводит к корреляции между сигналами $\{\mathbf{x}_p\}$. Другой частичный набор поддержки I_p является индивидуальным и не соответствует какой-либо корреляции.

Система использует «жадные» алгоритмы и стратегии слияния, консенсуса. Последняя стратегия состоит в том, чтобы выбрать для J_p индексы, которые присутствуют в наборах поддержки как минимум двух входящих соседних узлов.

Заключение.

Построена модель обработки сигналов в распределенных сенсорных сетях на основе разреженной аппроксимации. Модель может быть использована в различных приложениях робототехнических комплексов, таких как кодирование/декодирование информации в контуре управления, решения задач классификации и обработки изображений.

Литература

1. Eldar C., Kutyniok G. Compressed sensing: theory and applications. Cambridge University Press, 2012.

2. Foucart S., Rauhut H. A mathematical introduction to compressive sensing. Berlin: Springer, 2013.

УПРАВЛЕНИЕ РИСКАМИ В КОРПОРАТИВНЫХ СЕТЯХ

Тынкович Т.П.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ширинский В.П. – к.т.н., доцент

В работе проведен анализ защиты информации в корпоративных телекоммуникационных сетях.

На протяжении ряда лет во всех странах мира наблюдается тенденция стремительного развития корпоративных компьютерных телекоммуникационных сетей, современных мультимедийных средств и средств автоматизации.

С технологической точки зрения это - закономерное развитие методов использования новых информационных технологий в корпоративных сетях и на предприятиях.

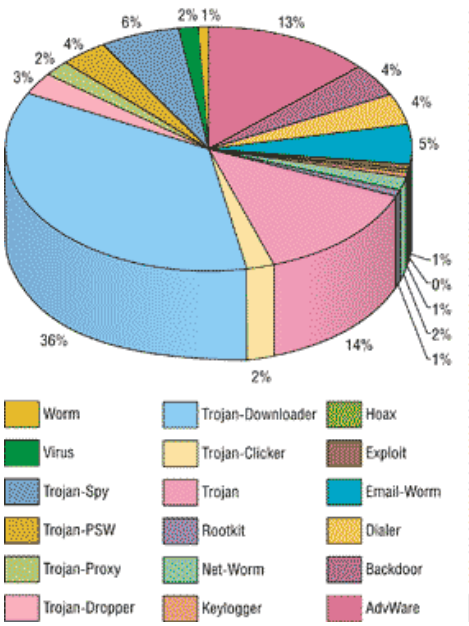
Возникновение всемирной компьютерной сети открыло возможность использования информационных ресурсов и интеллектуального потенциала практически любого предприятия. Использовать открывшиеся возможности это наверно, самая актуальная задача всех телекоммуникаций.

Корпоративная сеть большого предприятия может насчитывать сотни и тысячи компьютеров и, несмотря на технические меры защиты, весьма уязвима перед различными видами угроз. Как ни парадоксально это звучит, зачастую источником проблем являются пользователи ЛВС (локальных вычислительных сетей). Рассмотрим статистику инцидентов и несколько характерных случаев из практики.

Для анализа возьмем некоторые среднестатистические корпоративные сети, содержащие 500 компьютеров с электронной почтой и выходом в Интернет. Будем считать, что электронная почта идет через корпоративный почтовый сервер, защищенный одним из популярных в нашей стране антивирусов, например DrWeb, а выход в Интернет осуществляется централизованно через корпоративный прокси-сервер и Firewall. Анализ причин инцидентов приведено на рисунке 1.

Рисунок 1 – Причины инцидентов

Как видно из диаграммы, основной причиной всевозможных инцидентов являются вредоносные программы различных типов. В эту категорию попадают вирусы, программы категории Malware (шпионские программы, модули отображения рекламы и прочее нежелательное ПО). Очень часто появление вредоносного ПО напрямую связано с действиями пользователя. Анализ процентного состава вредоносного ПО приведено на рисунке 2.



AdvWare	2446
Backdoor	813
Dialer	760
Email-Worm	970
Exploit	129
Hoax	81
Keylogger	108
Net-Worm	320
Rootkit	140
Trojan	2512
Trojan-Clicker	405
Trojan-Downloader	6569
Trojan-Dropper	542
Trojan-Proxy	380
Trojan-PSW	698
Trojan-Spy	1169
Virus	286
Worm	153
Объем выборки ITW	18 481

Рисунок 2 – Типы вредоносных ПО

В ходе анализа типовых проблем, возникающих в локальной сети предприятия, многие из них невозможно решить чисто техническими средствами — необходим набор внутрикорпоративных регламентирующих документов. Основными из них являются положение о коммерческой тайне и положение о защите информации.

Положение о коммерческой тайне обычно содержит несколько типовых разделов:

- общие положения;
- основные понятия коммерческой тайны;
- защита коммерческой тайны;
- специальные обязанности лиц, допущенных к коммерческой тайне и отвечающих за защиту коммерческой тайны.

Типовое положение о защите информации может содержать четыре основных пункта:

- общие положения;
- требования к процессу разработки и к внедрению ПО собственной;
- требования к ПО сторонних разработчиков;
- обязанности персонала по обеспечению режима информационной безопасности при эксплуатации средств вычислительной техники, сетевых коммуникаций и программного;
- действия должностных лиц в случае нарушения режима информационной безопасности.

В данной статье рассмотрены проблемы, связанные с информационной безопасностью корпоративной сети. Основное внимание уделено реальным инцидентам, связанным с деятельностью пользователей. Следует отметить, что описанные нормативные документы часто рассматриваются администраторами сети как ненужная формальность, однако они являются очень важной составляющей в организации безопасности корпоративной сети, поскольку регламентируют поведение пользователей и их взаимодействие с администраторами. Без данного документа невозможно как таковое проведение служебных расследований и наказание пользователей за грубые нарушения правил работы в сети. Кроме того, наличие утвержденной политики информационной безопасности сводит к минимуму конфликтные ситуации между пользователями и администраторами сети, поскольку и те и другие действуют в рамках единых нормативных документов.

Список использованных источников:

1. Конеев, И.Р, Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с
2. Олифер В.Г. Олифер Н.А. Компьютерные сети 2ое издание / 123,779.
3. Майкл Коллинз Защита сетей. Подход на основе анализа данных.2019 с. 249-260..

АЛГОРИТМЫ КОНСЕНСУСА В БЛОКЧЕЙН СЕТЯХ

Яковчик Н.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Борискевич И.А. – к.т.н.,доцент

В работе проведен сравнительный анализ алгоритмов консенсуса применяемых в блокчейн сетях.

Консенсус – это достижение согласия по некоторому вопросу. Алгоритм консенсуса может определяться как механизм, с помощью которого блокчейн сеть достигает консенсуса. Публичные (децентрализованные) блокчейн сети построены как распределенные системы, и поскольку они не полагаются на центральные органы, распределенные узлы должны согласовывать валидацию транзакции. Алгоритм консенсуса в блокчейн сети [1] представляет собой набор определенных математических правил и функций, которые позволяют достичь соглашения между всеми участниками, т.е. позволяют выбрать того, кто может добавить новый блок транзакций в цепочку и, соответственно, обеспечить работоспособность сети. В настоящее время существует несколько различных методов достижения консенсуса.

PoW (Proof of Work) – является наиболее известным способом подтверждения транзакций. Чтобы участвовать в проверке транзакции, участникам необходимо публично доказать проведенную работу. Данный алгоритм решает сложную задачу по нахождению хэша (hash) [2], который соответствует определенным правилам. Первый, кто нашел правильную комбинацию, получает возможность добавить блок в цепочку. Основным недостатком является потребление большого количества электроэнергии всеми участниками сети, в которой применяется данный алгоритм.

PoS (Proof of Stake) – в данном алгоритме вероятность того, что участник добавит следующий блок транзакций в цепочку, определяется количеством монет участника. При этом каждый сетевой узел связан с определенным адресом, и чем больше монет принадлежит этому адресу, тем больше вероятность того, что этот узел сети намайнит следующий блок [3]. Злоумышленнику, который хочет совершить мошенническую транзакцию, потребуется владеть более 50% монет для надежной обработки нужных транзакций; покупка такого количества монет спровоцирует рост цен на них и сделает такую попытку чрезмерно дорогой.

PoET (Proof of Elapsed Time) – это механизм, который предотвращает использование больших вычислительных ресурсов и высокое потребление энергии. Концепция была изобретена в начале 2016 года компанией Intel. Каждый узел в блокчейне генерирует случайное время ожидания и переходит в спящий режим на указанный промежуток времени. Тот, кто выходит из спящего режима первым, – и есть тот участник, у которого самое короткое время ожидания. При выходе из спящего режима он включает новый блок в цепочку, передавая необходимую информацию всей одноранговой сети. Затем повторяется тот же процесс для обнаружения следующего блока.

PoC (Proof of Capacity) – этот алгоритм позволяет майнинг оборудованию использовать в сети доступное пространство на жестком диске для определения прав на майнинг вместо использования вычислительной мощности устройства.

PoB (Proof of Burn) – работает по принципу разрешения майнерам сжигать или уничтожать токены виртуальной валюты, что дает им право писать блоки пропорционально сгоревшим монетам. Майнеры должны предоставить доказательства того, что они сожгли несколько монет, то есть отправили их на проверяемый ненадежный адрес. Этот подход не потребляет никаких ресурсов.

PoI (Proof of Importance) – значимость каждого пользователя в сети определяется как количество средств, имеющихся у него на балансе, и количество проведенных транзакций с и на его кошелек. В отличие от более привычного PoS, который учитывает только баланс имеющихся средств у пользователя, PoI учитывает как количество средств, так и активность пользователя в блокчейн сети.

Самым распространенным алгоритмом консенсуса в настоящее время является PoW, который применяется в сети Bitcoin. При этом для майнинга требуются большие вычислительные мощности, что приводит к значительному потреблению электроэнергии [4]. Использование описанных выше механизмов консенсуса позволит уменьшить вычислительные затраты по сравнению с PoW.

Список использованных источников:

1. ЛелуЛ. Блокчейн от А до Я. Все о технологии десятилетия / ЛелуЛ. – Москва : Эксмо, 2018 – 256с.

2. Forklog: Что такое Proof-of-Work и Proof-of-Stake? [Электронный ресурс]. – Режим доступа: https://forklog.com/chto-takoe-proof-of-work-i-proof-of-stake/. – Дата доступа: 24.03.2020.

3. Medium: Какие алгоритмы консенсуса применяются в блокчейне [Электронный ресурс]. – Режим доступа: https://link.medium.com/WZRTTxQse5/. – Дата доступа: 25.03.2020.

4. 3DNews Daily Digital Digest: На майнинг биткоинов уходит больше электроэнергии, чем потребляет вся Швейцария. [Электронный ресурс]. – Режим доступа: https://3dnews.ru/990234/. – Дата доступа: 24.03.2020.

ЗАЩИТА КАНАЛОВ ПЕРЕДАЧИ И ХРАНЕНИЯ ДАННЫХ НА ОСНОВЕ АЛГЕБРАИЧЕСКИХ РЕШЕТЧАТЫХ КОДОВ

Алисеенко М.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Саломатин С.Б. – канд. тех. наук, доцент

Рассмотрены алгебраические решетки, задачи кратчайшего и ближайшего векторов решетки. Приведены выражения кратчайшего вектора решетки и порождающая матрица решетки. Рассмотрен алгоритм преобразования кратчайшего ортогонального базиса решетки.

Алгебраическая решетка является конечно порожденной аддитивной подгруппой множества R^n. Решетку L можно представить как множество целочисленных линейных комбинаций n линейно независимых базисных векторов в m-мерном евклидовом пространстве, где m и n – размерность и ранг решетки соответственно. Решетки, у которых размерность m и ранг n равны, называются полноразмерными [1]. Определитель решетки равен объему фундаментального параллелотопа, образованного базисом $B = b_1,\ldots,b_n$, рисунок 1. Базис решетки не единственен: матрица перехода от одного базиса решетки к произвольному другому унимодулярна, т. е. ее определитель равен ±1, поэтому детерминант решетки не зависит от выбора базиса [2]. Произведение базисной и унимодулярной матрицы даст новый базис решетки.

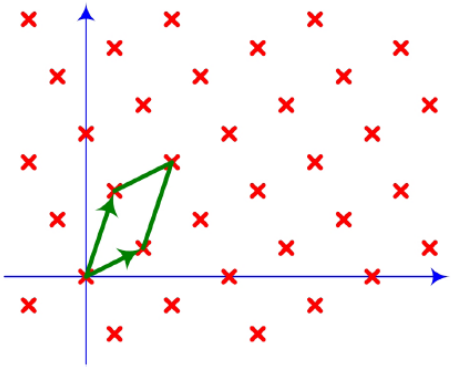


Рисунок 1 – Фундаментальный параллелотоп решетки, образованный базисом

Некоторые задачи теории решеток используются для создания схем стойкой криптографии, которые устойчивы для квантовых вычислений. Задача нахождения кратчайшего вектора (SVP, Shortest Vector Problem) подразумевает нахождение в заданном базисе решетки ненулевой вектор по отношению к определенной нормали. Математическая запись кратчайшего вектора:

$$a^* = \underset{a\in Z^n\setminus\{0\}}{\arg.\min}\|Aa\|^2 = \underset{a\in Z^n\setminus\{0\}}{\arg.\min} a^T G a, \quad (1)$$

где A – полноранговая матрица, являющаяся базисом решетки,

$G = A^T A$ – матрица Грамма решетки.

Задача нахождения ближайшего вектора (CVP, Closest Vector Problem) – нахождение вектора в решетке по заданному базису и некоторому вектору, не принадлежащему решетке, при этом максимально схожего по длине с заданным вектором. Математическая запись ближайшего вектора к произвольному вектору y:

$$a^* = \underset{a\in Z^n}{\arg.\min}\|Aa - y\|^2 = \underset{a\in Z^n}{\arg.\min}(a^T G a - 2y^T A a + y^T y). \quad (2)$$

По аналогии с линейными кодами решетка может быть выражена через порождающую матрицу и целочисленный коэффициент, что показано в выражении:

$$\Lambda = \{\lambda = \underbrace{[b_1 \vdots \cdots \vdots b_n]}_{G} a : a \in Z^n\}. \quad (3)$$

Под кратчайшим вектором решетки понимается вектор, длина которого:

$$\lambda(\Lambda) = \min_{x,y\in\Lambda, x\neq y}\|x - y\| = \min_{x\in\Lambda, x\neq 0}\|x\|. \quad (4)$$

Первый последовательный минимум, под которым понимается наименьший радиус окружности (шара), соответствует длине кратчайшего вектора решетки, рисунок 2.

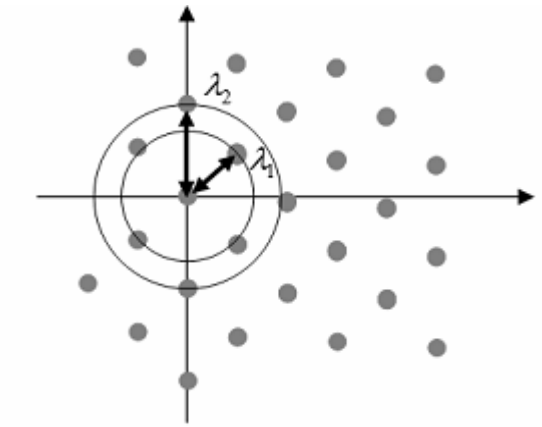


Рисунок 2 – Кратчайший базис-радиус решетки

Задачи теории решеток можно решить, если базис решетки редуцирован, т.е. состоит из относительно коротких почти ортогональных векторов. На сегодняшний день эффективным алгоритмом редукции базиса решетки является алгоритм LLL (Ленстры-Ленстры-Ловаса).

За полиномиальное время алгоритм преобразует базис на решетке в кратчайший почти ортогональный базис на этой же решетке. Для векторного пространства R^n процесс Грама-Шмидта позволяет преобразовать произвольный базис в ортонормированный («идеал», к которому стремится LLL-алгоритм), но не гарантирует того, что на выходе каждый из векторов будет целочисленной линейной комбинацией исходного базиса. Таким образом, полученный в результате набор векторов может и не являться базисом исходной решётки [3]. Необходима проверка на соблюдение условий нормы и Ловаса, при необходимости поменять местами вычисляемые векторы и пересчитать редуцированные векторы и их коэффициенты.

Алгоритм построения LLL-приведенного базиса делает $O(n^4 \log B)$ арифметических операций. При этом целые числа, встречающиеся в ходе работы алгоритма, имеют двоичную длину $O(n \log B)$ битов.

Список использованных источников:

1. Программный комплекс приведения базиса целочисленных решеток / О.В. Кузьмин, В.С. Усатюк // Программые продукты и системы №4, 2012. – С.180-183.

2. Использование ортогонализации Грама-Шмидта в алгоритме приведения базиса решетки для протоколов безопасности / А.В. Пискова, А.А. Менщиков,А.Г. Коробейников // Вопросы о кибербезопасности №1(14), 2016. – С.47-52.

3. Lattice Reduction / S. Galbraith // Mathematics of Public Key Cryptography, 2012. – P. 365-381.

МЕТОДИКА ОЦЕНИВАНИЯ ВРЕМЕННЫХ И ЧАСТОТНЫХ ХАРАКТЕРИСТИК ДИНАМИЧЕСКИХ СИСТЕМ

Бабак Е.В., Казак В.А., Левчук В.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Печень Т.М. – старший преподаватель

Предложена методика для исследования динамических систем в области критических значений степени покоя. Рассмотрены динамические системы в диапазоне критических значений степени демпфирования. Изучены количественные и качественные изменения временных и частотных характеристик систем.

Исследования динамических систем в области критических значений степени успокоения можно проводить по следующей методике:

– Получить передаточные функции колебательной и апериодической системы и соответствующие им выражения выходных сигналов при эквиваленте входного возникновения, а также сравнительной оценки расхождений выходных сигналов, амплитудночастотных (АЧХ) и фазочастотных (ФЧХ) характеристик системы.

– Решить следующую задачу: система второго порядка, трансформирующаяся из колебательной в апериодическую и наоборот из апериодической в колебательную, а модели выходных сигналов системы будут меняться, что приводит к возможным вариациям полюсов их передаточных функций и погрешностей оценивания ФЧХ и АЧХ, в частности, при реализации метода на основе парных переходных процессов [1]. В качестве такого примера может служить акселерометр линейных ускорений, работающих в диапазоне ускорений (перегрузок) с наложением значительных вибраций.

Передаточная функция системы 2-го порядка, описывается следующим уравнением [2]:

$$m\ddot{y} + D\dot{y} + cy = x(t) \quad (1),$$

где $x(t), y(t)$ − входной и выходной сигналы системы; m− инерционная масса системы; D − коэффициент демпфирования системы; m − жесткость подвесов системы, можно представить в виде

$$W(S) = (S^2 + 2\varepsilon\omega_0 S + \omega_0^2)^{-1} \quad (2),$$

где $\varepsilon = D/(2\omega_0)$ − степень успокоения системы; $\omega_0 = \sqrt{c/m}$− собственная частота системы.

Полюсы передаточной функции можно найти из уравнения:

$$S^2 + 2\varepsilon\omega_0 S + \omega_0^2 = 0$$

решая его относительно S:

$$S_{1,2} = -\varepsilon\omega_0 \pm \sqrt{\varepsilon^2\omega_0^2 - \omega_0^2} = \omega_0(-\varepsilon \pm \sqrt{\varepsilon^2 - 1}) \quad (3),$$

При $\varepsilon < 1$полюсы S_1 и S_2− комплексные числа, и система – колебательная.

При $\varepsilon > 1$полюсы S_1 и S_2−действительные числа, и система – апериодическая.

– Сравнить эти системы по выходным сигналам, являющимся реакцией на импульсное входное воздействие.

– Проанализировать расчетные данные на предмет изменения поведения системы. Следует учитывать, что при изменении степени успокоения системы за счет различных факторов в области, близкой к критической, может измениться поведение системы, а значит, могут измениться полюсы передаточной функции.

Таким образом, динамические характеристики систем представляют собой функции не только частот, воздействующих сигналов или их составляющих, но и условий применения систем, что приводит как к количественным, так и качественным изменениям временных и частотных характеристик систем. Для того, чтобы учесть количественные изменения следует воспользоваться известными статистическими приемами оценивания погрешностей характеристик систем, вызванных влияющими величинами, или определяя набор характеристик для фиксированных интервалов влияющих величин.

Список использованных источников:

1. Бойков И.В., Кривулин Н.П. Методы идентификации динамических систем // Программные системы: теория и приложения. 2014. Т. 5. № 5– 2(23). С. 79– 96.

2. Гарькина И.А., Данилов А.М., Тюкалов Д.Е. Сложные системы: идентификация динамических характеристик, возмущений и помех // Современные проблемы науки и образования. 2015. № 1. Ч. 1. С. 88.

БЕЗОПАСНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ В СЕТЯХ 4G/LTE

Белянков Д. А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Цветков В. Ю. – д. т. н., доцент

В работе рассмотрена беспроводная технология 4G/LTE и проблемы, связанные с обеспечением ее безопасности и конфиденциальности.

За последние несколько десятилетий мобильные системы стали незаменимыми для выполнения пользователями своих повседневных задач. Это привело к быстрому развитию беспроводных технологий таких как 2G, 3G, 4G и 5G для мобильных сетей. Беспроводная технология 4G была изобретена для улучшения качества широкополосной связи и обеспечения возможности использования мультимедийных программ.

Существуют множество технологических достижений, которые обеспечивают беспроводные сети 4G/LTE по сравнению с более ранними технологиями. Во-первых, мобильные системы 4G/LTE отлично работают, используя модель TCP/IP. Это фактически снижает финансовые и вычислительные затраты, когда портативные устройства могут подключаться к интернету с использованием интернет-протокола (IP) без каких-либо ограничений для ранее закрытых сотовых конфигураций. Тем не менее, благодаря широкому разнообразию протоколов связи, включенных в модель TCP/IP, беспроводные сети 4G/LTE сталкиваются с множеством проблем безопасности и конфиденциальности.

Ключевые проблемы для обеспечения безопасности беспроводных сетей 4G/LTE можно обобщить в трех аспектах. Во-первых, мобильные устройства могут выходить в Интернет из любого места и поэтому уязвимы для взлома различными продвинутыми постоянными угрозами (APT). Во-вторых, хотя мобильные системы на базе IP регулярно обновляются с помощью криптографических механизмов и механизмов безопасности, это влияет на их производительность и пропускную способность обработки трафика, что требует безопасных и обновленных стандартов и архитектур беспроводной связи. И третье, хотя производители выпускают новые поколения технологий 4G/LTE, они не регулярно разрабатывают новые стандарты для смягчения уязвимостей и сдерживания роста кибер-угроз.

Международный союз электросвязи (ITU) объявил Международный стандарт усовершенствованной подвижной электросвязи (IMT-Advanced) для беспроводных сетей 4G. Беспроводная технология 4G включает следующие критерии: высокая скорость передачи данных, которая составляет 100 Мбит/с для мобильных устройств и 1 Гбит/с для компьютерных устройств, высокое качество обслуживания (QoS) и высокая скорость работы сети и ее покрытие.

Архитектура LTE включает в себя модули, необходимые для установки сетевых протоколов между базовыми станциями и мобильными системами. Архитектура включает в себя три модуля: пользовательское оборудование (UE), универсальная наземная сеть радиодоступа (E-UTRAN) и улучшенное пакетное ядро (EPC). Оборудование пользователя, например, ноутбуки или смартфоны, могут подключаться к беспроводной сети через развитый узел NodeB (eNodeB), используя базовые станции E-UTRAN. ENodeB использует некоторые сетевые протоколы доступа для обмена сообщениями с UE. E-UTRAN связывается с EPC, который является инфраструктурой на основе IP, в то время как EPC связывается с поставщиком проводной IP-сети.

Контроль безопасности 4G/LTE. Уровни абстракции вставляются в архитектуру 4G/LTE в виде уникальных идентификаторов (ID) для смартфонов (т. е. UE). Временный уникальный идентификатор используется на SIM-карте для предотвращения кражи идентификаторов злоумышленниками. Другим методом улучшения безопасности 4G является добавление защищенного выделения между UE и MME. Хотя для беспроводной технологии 4G/LTE используется несколько элементов управления безопасностью, ее дизайн, основанный на архитектуре с открытым IP-адресом, и изощренность хакеров APT затрудняют безопасность и конфиденциальность систем 4G/LTE.

Для обеспечения безопасности мобильных устройств, использующих беспроводные технологии 4G/LTE, должна быть обеспечена защита соединений между UE и MME, а также между элементами проводных сетей и мобильными станциями. Удовлетворения этих требований безопасности 4G/LTE можно добиться путем добавления расширенной иерархии ключей, длительной аутентификации и согласования ключей и дополнительной безопасности взаимодействия для сетевых элементов. Требования подразделяются на ключевые блоки и сквозную безопасность LTE.

Ключевые блоки включают в себя следующие элементы [1]:

- Ключ безопасности и иерархии. LTE имеет пять ключевых стратегий, используемых для соединений EPS и E-UTRAN. Ключи объявляются следующим образом: ключи шифрования и целостности KANS используются для защиты трафика без доступа (NAS) между UE и MME, шифрование KUP используется для шифрования трафика между UE и eNodeB и ключи шифрования и целостности KPRC используются для защиты управления радиоресурсами (RRC) между UE и eNodeB.

- Ключевой менеджмент. Управление ключами LTE включает в себя три функции: создание, распространение и генерация ключей. Важно, чтобы беспроводная технология 4G/LTE имела механизмы управления ключами, которые предотвращают кражу ключей, поскольку мобильные устройства с инфраструктурой на основе IP могут часто получать доступ к различным беспроводным сетям.

- Аутентификация, шифрование и защита целостности. LTE зависит от использования регулярного обновления процесса аутентификации путем обмена порядковыми номерами в сообщениях механизмов шифрования. Протокол IPsec и туннели также используются для обеспечения конфиденциальности данных пользователей при передаче трафика между узлами LTE.

- Уникальные идентификаторы пользователей. LTE имеет несколько механизмов идентификаторов пользователей, которые мешают злоумышленникам изучать идентификационные данные мобильных пользователей. Механизмы идентификаторов содержат следующее: международный идентификатор мобильного оборудования (IMEI), который является постоянным уникальным идентификатором для каждой мобильной станции, M-TMSI, который является временным идентификатором, который определяет UE внутри MME, и временный идентификатор сотовой радиосети (C-RNTI), который является уникальным и временным идентификатором UE.

Комплексная безопасность LTE включает в себя следующие элементы [2]:

- Соглашение об аутентификации и ключе (AKA). Основой безопасности LTE является аутентификация UE и беспроводных сетей. Это может быть достигнуто с использованием AKA процесса, который утверждает, что обслуживающая сеть аутентифицирует личность пользователя, а UE сертифицирует сетевую подпись. AKA создает ключи шифрования и целостности, применяемые для создания различных сеансовых ключей.

- Конфиденциальность и целостность сигнализации. Безопасность плоскостей управления сетевым доступом достигается, когда сигнализация уровня RCC и NAS зашифрована и защищена целостность. Защита шифрования и целостности сигнализации LTE RRC выполняется на уровне протокола конвергенции пакетных данных (PDCP), тогда как уровень NAS обеспечивает защиту путем шифрования сигнализации уровня NAS. Эта защита не может быть уникальным образом выполнена для каждого соединения UE, но она выполняется через доверенные соединения между AGW и eNodeB.

- Конфиденциальность плоскости пользователя. LTE имеет функцию безопасности для плоскости пользователя посредством шифрования данных / голоса между UE и eNodeB. Шифрование выполняется на уровне IP с использованием основанных на IPsec туннелей между AGW и eNodeB, но из-за соображений производительности и эффективности защита от проникновения на уровне пользователя не обеспечивается.

Кроме всего прочего беспроводная технология 4G/LTE сталкивается с различными типами кибератак, которые могут повлиять на целостность, конфиденциальность, доступность и аутентификацию: атаки против конфиденциальности данных мобильных пользователей пытаются раскрыть конфиденциальные данные / мультимедиа пользователей; атаки против целостности пытаются изменить обмен данными между точками доступа 4G и мобильными пользователями. Механизмы аутентификации и сохранения конфиденциальности с хэш-функциями широко используются для защиты беспроводных сетей 4G от атак целостности; атаки против аутентификации пытаются нарушить процесс аутентификации клиент-сервер и/или сервер-клиент; атаки на доступность пытаются сделать недоступными такие службы, как служба маршрутизации данных. Для защиты от этих атак обычно используются брандмауэры и системы обнаружения вторжений.

Несмотря на большое количество научно-технических исследований и разработок, которые были проведены для обеспечения безопасности беспроводных сетей 4G / LTE, существует несколько проблем, которые должны быть в центре внимания исследователей, а именно: разработка гибкой и масштабируемой архитектуры 4G/LTE, которая может решать проблемы безопасности, так как существует множество устройств и систем, которые обычно связаны с сетями 4G, что приводит к уязвимостям и лазейкам в сетях; обнаружение DoS-атак, которые пытаются нарушить беспроводные сети 4G, поскольку хакеры часто создают новые сложные варианты против eNodeB, UE и прерывистых служб приема; отслеживание местоположения означает отслеживание присутствия UE в определенной ячейке; существуют технические пробелы в вопросах масштабируемости сети, безопасности и конфиденциальности с помощью SDN.

Список использованных источников:0

1 Mohapatra SK, Swain BR, Das P Comprehensive survey of possible security issues on 4G networks. I0nt J Netw Secur Appl.2015. – 62.

2. Ferrag MA, Maglaras L, Argyriou A, Kosmanos D, Jan-icke H Security for 4G and 5G cellular net-works: a survey of existing authentication and privacy-preserving schemes. J Netw Comput Appl. 2017. – 55–82.

МОДУЛЯТОР МАХА-ЦЕНДЕРА

Бушило В.Н.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Тарченко Н.В. – канд. техн. наук

Современные высокоскоростные системы передачи сигналов по оптическим волокнам основаны на применении спектрального разделения каналов – технологии DWDM. В процессе проектирования данных систем необходимо выбрать оптимальный метод модуляции. Основным элементом формирования высокоскоростных сигналов является внешний оптический модулятор. Одним из вариантов исполнения внешнего модулятора является электрооптический модулятор Маха-Цендера.

Электрооптический модулятор Маха-Цендера предназначен для модуляции излучения мощного оптического лазера. Структурная схема данного модулятора представлена на рисунке 1. Непрерывное излучение лазера E_0 Y-разветвителем направляется по двум каналам (плечам интерферометра). Далее в каждом из каналов Y_1 и Y_2 непрерывное световое излучение попадает в фазовые модуляторы, которые позволяют изменять показатель преломления волновода пропорционально напряжению U_1 и U_2. На выходе сдвинутые по фазе сигналы складываются в процессе интерференции, получая E_{out}.

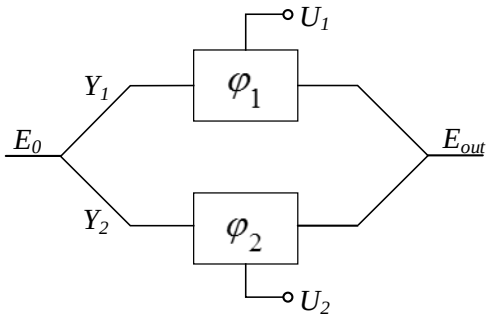


Рисунок 1 – Схема модулятора Маха-Цендера

Выходное значение E_{out} принимает следующий вид:

$$E_{out} = \frac{E_0}{2}\left(e^{j\varphi_1(t)} + e^{j\varphi_2(t)}\right), \quad (1)$$

где E_0 – входное оптическое излучение; $\phi_1(t)$ и $\phi_2(t)$ – сдвиги фаз в верхнем Y_1 и нижнем Y_2 плечах.

Формирование фазового сдвига связано с изменением управляющего напряжения

$$\varphi_1(t) = \frac{U_1(t)}{V_{\pi 1}}\pi, \quad \varphi_2(t) = \frac{U_2(t)}{V_{\pi 2}}\pi. \quad (2)$$

Существует два режима работы модулятора Маха-Цендера. В режиме “push-push” в обоих плечах модулятора формируется одинаковый фазовый сдвиг $\phi(t) = \phi_1(t) = \phi_2(t)$ (например, при $U_1(t) = U_2(t) = U(t)$ и $V_{\pi 1} = V_{\pi 2} = V_\pi$), что позволяет осуществлять фазовую модуляцию. При этом амплитуда входного сигнала не изменяется. В режиме “push-pull” обоих плечах формируется одинаковый по величине, но разный по знаку фазовый сдвиг $\phi_1(t) = -\phi_2(t)$ (например, при $U_1(t) = -U_2(t) = U(t)/2$ и $V_{\pi 1} = V_{\pi 2} = V_\pi$), что приводит к чистой амплитудной модуляции.

Таким образом, модулятор Маха-Цендера позволяет осуществлять как фазовую, так и амплитудную модуляцию, что позволяет использовать его в качестве универсального базового элемента в схемах формирования различных форматов модуляции в современных высокоскоростных оптических системах передачи.

Список использованных источников:

1. High-order modulation for optical fiber transmission / Dr. Matthias Seimetz // Springer, 2009. – 247 с.

2. Передача сигналов модуляции интенсивности света в аналоговых волоконно-оптических линиях связи / Щербаков В.В., Солодков А.Ф., Задерновский А.А. // Журнал: Радиоэлектроника. Наносистемы. Информационные технологии, 08.06.2016. – 23 с.

СПОСОБЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЯХ ПЕРЕДАЧИ

Дудак М.Н.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Урядов В.Н. – к.т.н., доцент

Долгое время считалось, что волоконно-оптические линии передачи (ВОЛП) обладают максимальной защищенностью и скрытностью информации, но современные исследования показали, что есть множество способов для съема лазерного излучения с оптических линий, и доказали, что существует потенциальная угроза нарушения конфиденциальности передаваемой информации по ВОЛП.

В свете бурного развития ВОЛП на магистральных, городских, корпоративных и внутриузловых сетях все больше уделяется внимания вопросам защиты информации. Под защитой информации понимается комплекс организационных и технических мер по предотвращению угроз информационной безопасности и устранению их последствий. При защите информации в ВОСП можно выделить защиту информации от расшифровки и защиту оптического сигнала от физического снятия.

В первом случае используются как криптографические методы, так и защита оптического сигнала от дешифровки на физическом уровне (когерентные, поляризационные ил спектральные методы передачи информации в ВОСП). Во втором случае происходит защита оптического сигнала от снятия либо путем его отвода с волоконных световодов оптического тракта, либо же путем попыток отвода и соответственно пресечения этих попыток. Поскольку отвод мощности с кабеля можно организовать разными методами, то и способов осуществления снятия информации, несанкционированного доступа (НСД) существует несколько.

Существует три способа осуществления НСД:

- разрывной способ;
- безразрывный без принудительного отвода мощности;
- безразрывный с принудительным отводом мощности.

В разрывном способе аппаратура злоумышленника, отводящая мощность с оптоволокна (приемник перехвата), внедряется в намеренно созданный разрыв оптического кабеля, с которого осуществляется съем информации. Для осуществления съема оптической мощности волоконно-оптический кабель подвергается разрыву. Затем с помощью сварки его концы соединяются с волоконно-оптическим разветвителем, который таким образом оказывается включенным в разрыв. Хотя этот способ и позволяет эффективно осуществлять НСД, реализация его сопряжена с рядом трудностей. Работы по разрыву волокна и сварке его концов с разветвителем очень сложно выполнить в кратчайшие сроки, да и сам разрыв кабеля не останется не замеченным.

Высокий уровень защиты в данном случае можно получить при использовании специализированных оптических кабелей, которые спроектированы таким образом, что резко усложняет технологию съема данных с волокон и позволяет фиксировать внешние воздействия (с помощью электромагнитного поля, газа, закаченного в данный кабель и т.д.).

Отличные результаты дает рефлектометрический анализ линии, при котором любое вмешательство в кабель, появление в нем сварных соединений, вставок и т.д., вызывает неоднородности.

Таким образом, НСД, выполненный таким способом, может быть достаточно легко обнаружен и проконтролирован с помощью аппаратуры оптической рефлектометрии. Методы, позволяющие обнаружить такой метод такой НСД, известны и эффективны. Вероятность применения такого метода при вероятной использовании НСД мала.

Во втором способе для съема информации используется излучение, возникающее естественным образом в результате рассеяния света на муфтах, соединителях, устройствах ввода и вывода оптической мощности, а также на самом оптическом волокне. Все эти устройства вносят в линию дополнительные потери. Оптическая мощность, теряемая на них, частично излучается с них в окружающую среду. Мощность этих вытекающих мод излучения применяется для осуществления НСД, применяя при этом различные системы сбора мощности, чаще всего линзовые.

Большое достоинство данного способа в том, что за счет использования излучения, которое существует независимо от того есть НСД или нет, его практически невозможно проконтролировать системами мониторинга состояния линии. Данный режим позволяет

организовать режим «прозрачности» НСД, когда ВОСП «не замечает» отбор оптического сигнала. Рефлектометрические системы не покажут каких-либо изменений и неоднородностей в волоконно-оптическом тракте, потому что их нет, а системы не обнаружат дополнительных потерь.

Однако борьба против съема информации в данном случае является достаточно эффективной и довольно простой. Число участков возникновения вытекающего излучения известно и ограничено, что и позволяет организовать на них постоянную охрану и наблюдение, либо применять какие-либо другие организационно-технические мероприятия.

Соединительные устройства и сами волоконные световоды постоянно совершенствуются, снижаются потери в самом волокне, следовательно, уменьшается мощность рассеиваемого излучения. Мощности, которые теряются в каких-либо точках, уже оказываются недостаточные для работы приемника НСД, и приходится организовывать ее сбор с довольно протяженного участка кабеля.

Поэтому организация НСД этим способом маловероятна, поскольку меры противодействия для этого случая хорошо известны и отработаны.

В третьем способе пытаются добиться изменения его оптических свойств путем какого-либо воздействия на волоконный световод, что и приводит к выводу части излучения из световода.

Если той мощности, которая излучается с волокна на каком-либо участке, оказывается недостаточно для организации НСД, то надо сделать так, чтобы мощности на этом участке излучалось больше.

Чтобы осуществить отвод оптического информационного сигнала с кабеля на каком-либо участке, используется локальное воздействие на его волоконные световоды. При таком воздействии изменяются их оптические свойства, что и приводит к вытеканию сигнала. Методы воздействия на волокно:

- изгиб волокна;
- изменение диаметра волокна;
- микроизгибы волокна;
- акустическое воздействие на волокно;
- воздействие химическими реактивами.

Из этих методов наиболее распространенным и наиболее интересным является метод изгиба волокна, потому что он позволяет организовать направленный вывод излучения. При изменении диаметра световода, а также акустическом или химическом воздействии вышедшее излучение распространяется по многим направлениям и труднее поддается сбору. В случае же изгиба вышедшее излучение распространяется вдоль одного направления, поэтому оно может быть собрано при помощи различных линзовых систем. Вот почему изгиб волокна является популярным вариантом осуществления НСД.

Достоинством данного метода является высокая эффективность. Ведь изменяя радиус изгиба волокна можно добиться снятия таких величин оптической мощности, при которых будет достаточно для перехвата информации. Однако «прозрачным» данный метод назвать нельзя, поскольку мощность отводится принудительно, то и подключение вызовет снижение уровня мощности на приемной стороне линии. Поэтому основным методом обнаружения данного НСД способа является контроль над уровнем мощности на приемной стороне. Если устройство контроля обнаруживает ее снижение, то оно делает вывод о наличии НСД к линии.

Итак, данная система контроля хотя и позволяет обнаружить факт НСД, но очень эффективным методом не является не является. Поэтому можно считать, что для осуществления НСД берется именно этот способ, предлагающий изгиб волокна для отвода мощности. Разработка эффективных методов и систем обнаружения НСД для этого случая является актуальной научно-технической проблемой.

Но все же система контроля, действующая по описанному выше варианту, позволяет бороться с НСД. Очевидно, что ее эффективность будет зависеть от ряда параметров, таких как величина отводимой мощности, чувствительность фотоприемников, и, если попробовать их проанализировать, то на основании такого анализа работу системы можно оптимизировать, сведя к минимуму ее ложные срабатывания.

Основная идея повышения эффективности данного метода контроля состоит в том, чтобы постараться принять такие меры, которые заставили бы нарушителя увеличит уровни отводимой оптической мощности. Ведь это, в свою очередь, создаст более благополучные условия для обнаружения.

Существует множество исследований, посвященных проблеме НСД в традиционных, электрических линиях связи. В них для защиты от НСД предлагается использовать различные методы кодирования, затрудняющие расшифровку информации в случае малых уровней сигнала, но в тоже время не влияющие на прием, если уровни сигнала большие.

Список использованных источников:

1. Фриман Р. Волоконно-оптические системы связи. – М.: Техносфера, 2003.

2. Мировицкий Д. И., Будагян И. Ф., Дубровин В. Ф. Микроволноводная оптика и голография.— М.: Наука. Главная редакция физико-математической литературы, 1983.

3. Гришачев В.В., Кабашкин В.Н., Фролов А.Д. Информационное противодействие угрозам терроризма № 4 (2005)

СПОСОБЫ ОБЕПЕЧЕНИЯ ВЫСОКОЙ ДОСТУПНОСТИ КЛАСТЕРНЫХ СЕРВИСОВ

Жук П.Б.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бобов М.Н. – доктор технических наук, профессор

В данной работе приведено определение высокой доступности кластерных сервисов, основные критерии высокой доступности и рассмотрены способы достижения высокой доступности в кластерных сервисах.

Высокая доступность – это характеристика системы, отражающая ее длительную бесперебойную работ близкую к 100% работоспособности в течение всего времени работы системы.

Критерием высокой доступности является время простоя. Время простоя - это период времени, когда система недоступна для использования или не отвечает.

Доступность может быть измерена как процент времени, в течение которого сервис доступен:

$$x = ((n - y) * 100) / n,$$

где n - общее количество времени работы системы, y - общее количество времени, в течение которых сервис был недоступен.

Добавление большего количества компонентов в систему не приводит к большей стабильности и обеспечивает высокую доступность: это может привести к обратному, так как большее количество компонентов увеличивает вероятность отказов.

Существует два подразделения мероприятий для обеспечения высокой доступности сервиса: конфигурация кластера в целом и конфигурация отдельного узла.

Мероприятия по конфигурации кластера для обеспечения высокой доступности включают в себя методики по балансировке нагрузки между узлами и резервирование:

- Active/active – нагрузка распределяется между двумя узлами для обеспечения их большей отказоустойчивости. По своей сути является кластером из двух узлов.
- Active/passive — каждый узел имеет полное резервирование. Резерв включается в работу только тогда, когда отказывает соответствующий основной узел. Резерв может быть горячим или холодным в зависимости от необходимой конфигурации.
- N + 1 – на группу узлов в кластере N приходится один резервный узел, который заменяет место отказавшего узла.
- N + M – является логическим продолжением метода N + 1, только количество резервных узлов равно M > 1.
- N - к - 1 – позволяет резервному узлу включаться в работу временно, пока отказавший узел не будет восстановлен, после чего исходная нагрузка возвращается на основной узел для сохранения исходного уровня доступности системы.
- N - к - N – это сочетание active / active и N + M кластеров. В N - к - N кластере соединения от отказавших узлов перераспределяются между остальными активными узлами. Тем самым устраняется необходимость отдельного резервного узла, но при этом все узлы кластера должны обладать некоторой избыточной мощностью сверх минимально необходимой.

Мероприятия по конфигурации отдельного узла кластера для обеспечения высокой доступности включают:

- Резервирование и репликацию дисков: отказ части внутренних дисков не приводит к сбоям системы.
- Резервирование внешних сетевых соединений: повреждения кабеля, отказ коммутатора или сетевого интерфейса не приводят к полному отключению от сети.
- Резервирование внутренних соединений сети хранения данных (SAN): повреждения кабеля, сбой коммутатора или сетевого интерфейса не приведут к потере соединения серверов с хранилищем (это нарушило бы неразделяемую архитектуру).
- Избыточные схемы электропитания различного оборудования, как правило, защищённого источниками бесперебойного питания, и резервируемые блоки питания.

1. Research on High Availability Architecture of Cloud Platform / Lai Xinming, Wang Haitao, Zhao Jing, Zhang Fan, Zhao Chao and Wu Gang // https://iopscience.iop.org/article/10.1088/1742-6596/1345/2/022044
2. *Blueprints for High Availability / E. Marcus, H. Stern // Wiley Publishing, Inc., 2003. – P. 9-17*
3. High Availability with Clusters of Web Services / Julio Fernández Vilas, José Pazos Arias, Ana Fernández Vilas // https://www.researchgate.net/publication/221240361_High_Availability_with_Clusters_of_Web_Services, 2004.

ПРОТОКОЛ MQTT-SN

Каптюг Д.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Хацкевич О.А.– канд. тех. наук

В данной работе будут подробно рассмотрены архитектура и формат сообщений протокола MQTT-SN.

MQTT (Message Queue Telemetry Transport) – это открытый протокол обмена данными созданный для передачи данных на удалённых локациях, где требуется небольшой размер кода и есть ограничения по пропускной способности канала. Вышеперечисленные достоинства позволяют применять его в системах M2M и IIoT.

Архитектура протокола MQTT-SN. На рисунке 1 показыны три компонента MQTT-SN, MQTT-SN клиенты, MQTT-SN шлюзы и серверы пересылки MQTT-SN. Клиенты MQTT-SN подключаются к серверу MQTT через MQTT-SN шлюзы, используя протокол MQTT-SN. MQTT-SN шлюз может интегрирован или не интегрирован с сервером MQTT. В случае автономного шлюза протокол MQTT используется между сервером MQTT и шлюзом MQTT-SN. Его основная функция - передача данных между MQTT и MQTT-SN. Клиенты MQTT-SN также могут получить доступ к шлюзам через сервер пересылки, если шлюз не подключен напрямую к своей сети. Сервер пересылки инкапсулирует кадры MQTT-SN, которые он принимает со стороны клиента, и передает их без изменений шлюзам; в обратном направлении он декапсулирует кадры, которые он получает от шлюза, и отправляет их клиентам, также без изменений.

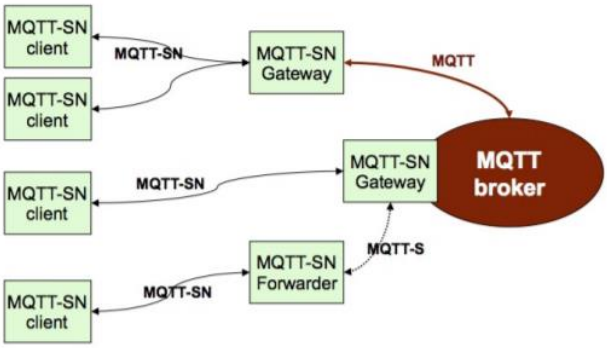


Рисунок 1 – Архитектура MQTT-SN

В зависимости от того, как шлюз выполняет трансляцию протокола между MQTT и MQTT-SN, мы можем различать два типа шлюзов, а именно прозрачные и агрегирующие шлюзы.

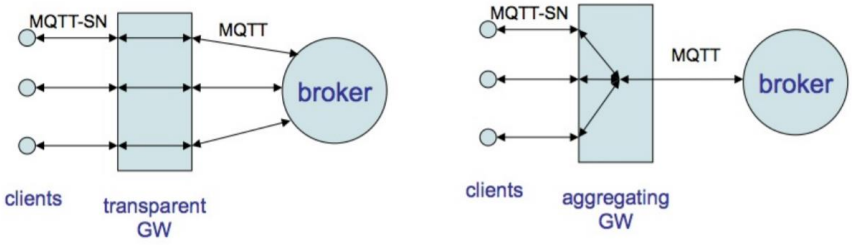


Рисунок 2 – Прозрачный и агрегирующий шлюзы

Для каждого подключенного клиента MQTT-SN прозрачный шлюз будет устанавливать и поддерживать соединение MQTT с сервером MQTT. Это MQTT-соединение зарезервировано исключительно для сквозного обмена сообщениями между клиентом и сервером. Между шлюзом и сервером будет столько же соединений MQTT, сколько клиентов MQTT-SN подключено к шлюзу. Поскольку все обмены сообщениями являются сквозными между клиентом MQTT-SN и сервером MQTT, все функции, которые реализуются сервером, могут быть предложены клиенту. Важным условием для реализации прозрачного шлюза сервер MQTT является поддержка отдельного соединения для каждого активного клиента. Некоторые реализации сервера MQTT могут

накладывать ограничение на количество одновременных подключений, которые они поддерживают.

Агрегирующий шлюз вместо подключения MQTT для каждого подключенного клиента будет иметь только одно подключение MQTT к серверу. Все обмены сообщениями между клиентом MQTT-SN и агрегирующим шлюзом заканчиваются на самом шлюзе. Затем шлюз решает, какая информация будет передана на сервер.

Передаваемые сообщения имеют общий формат, показанный на рисунке 3.

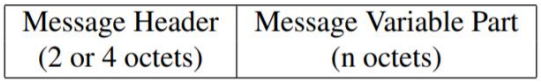


Рисунок 3 – Общий формат сообщений протокола MQTT-SN

Сообщение MQTT-SN состоит из двух частей: длинный заголовок длиной 2 или 4 октета и необязательная переменная часть. Заголовок присутствует всегда и содержит одни и те же поля, наличие и содержание переменной части зависят от типа рассматриваемого сообщения.

Список использованных источников:

1. MQTT For Sensor Networks (MQTT-SN) Protocol Specification // Andy Stanford-Clark and Hong Linh Truong, November 14, 2013.

АРХИТЕКТУРА ПРОТОКОЛА SNMP

Ковятинец И.П.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бобов М.Н. – д.т.н., профессор

В данной работе рассматриваются принципы протокола SNMP, а также алгоритмы работы и описание операций в данном протоколе.

SNMP (Simple Network Management Protocol) – протокол уровня приложений для управления устройствами в IP-сетях на основе архитектур TCP/UDP. Протокол SNMP позволяет управлять узлами, такими как серверы, рабочие станции, маршрутизаторы, коммутаторы и устройства безопасности, в сети IP. Он позволяет сетевым администраторам контролировать работу сети, выполнять поиск и разрешение сетевых проблем, а также планировать рост сети.

Система SNMP состоит из трёх элементов:

– диспетчер SNMP;
– агенты SNMP (управляемый узел);
– информационная база управления (MIB).

Диспетчер SNMP является частью системы управления сетями (network management system — NMS). Он запускает ПО для управления SNMP. Диспетчер SNMP может собирать данные от агента SNMP с помощью запроса get и изменять настройки на агенте с помощью запроса set. Кроме того, агенты SNMP могут пересылать информацию непосредственно в NMS с использованием уведомлений («ловушек», trap).

Схематическое представление алгоритма работы протокола приведено на рисунке 1.

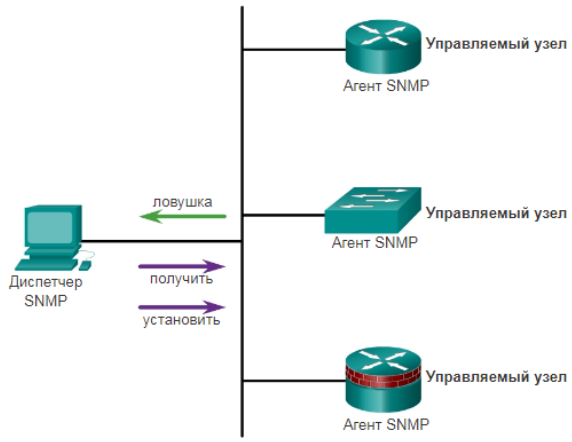


Рисунок 1 – Схема работы алгоритма SNMP

Агент SNMP и MIB размещены на клиентах сетевого устройства. Сетевые устройства, которыми необходимо управлять, такие как коммутаторы, маршрутизаторы, серверы, межсетевые экраны и рабочие станции, оборудованы программным модулем агента SMNP. В базах MIB хранятся данные о работе устройств; они должны быть доступны для прошедших проверку подлинности удалённых пользователей. Агент SNMP отвечает за предоставление доступа к локальной базе объектов MIB, которая содержит сведения о ресурсах и активности.

SNMP определяет способ обмена информацией об управлении между приложениями управления сетями и агентами управления. SNMP использует UDP, номер порта 162, для получения и отправки информации по управлению.

Агенты SNMP, размещенные на управляемых устройствах, собирают и сохраняют информацию об устройстве и его работе. Агент хранит эти сведения локально в базе MIB. Затем диспетчер SNMP использует агент SNMP для доступа к сведениям, хранящимся в базе MIB.

Существует два основных запроса диспетчера SNMP — get и set. Запрос get используется системой управления сетью NMS для отправки на устройство запроса о получении данных. Запрос set используется системой управления сетью NMS для изменения переменных настройки в устройстве агента. Запрос set также может инициировать определённые действия с устройством. Например, запрос set может вызвать перезагрузку маршрутизатора, отправку конфигурационного

файла или получение конфигурационного файла. Диспетчер SNMP использует запросы get и set для выполнения операций.

Описание операций представлено в таблице 1.

Таблица 1 – Описание операций протокола SNMP

Операция	Описание
get-request	Получает значение из определенной переменной.
get-next-request	Получает значение из переменной в таблице; Диспетчер SNMP не обязательно должен знать точное имя переменной. Чтобы найти необходимую переменную в таблице, выполняется последовательный поиск в таблице.
get-bulk-request	Получает большие блоки данных, например несколько строк в таблице, что обычно требует передачи многочисленных небольших блоков данных.
get-response	Отвечает на запросы get-request, get-next-request и set-request, отправляемые системой NMS.
set-request	Сохраняет значение в определенной переменной.

Агент SNMP отвечает на запросы диспетчера SNMP следующим образом:

Получение переменной MIB. Агент SNMP выполняет эту функцию в ответ на запрос GetRequest-PDU от системы NMS. Агент получает значение запрошенной переменной MIB и передаёт это значение системе NMS.

Установка переменной MIB. Агент SNMP выполняет эту функцию в ответ на запрос SetRequest-PDU от системы NMS. Агент SNMP изменяет значение переменной MIB на значение, определённое системой NMS. Ответ агента SNMP на запрос set включает новые параметры в устройстве.

Существует несколько версий SNMP:

– SNMPv1 — простой протокол управления сетями, полноценный стандарт Интернета, описанный в документе RFC 1157;

– SNMPv2c — описан в серии документов RFC 1901—1908; использует среду администрирования на базе строки сообщества;

– SNMPv3 — обеспечивающий взаимодействие протокол на основе стандартов, первоначально определённый в серии документов RFC 2273—2275; обеспечивает защищённый доступ к устройствам с помощью аутентификации и шифрования пакетов в сети. Данная версия протокола включает следующие функции обеспечения безопасности: контроль целостности сообщений для защиты пакетов от искажения при пересылке; аутентификация для подтверждения достоверности источника сообщения и шифрование для предотвращения прочтения содержимого сообщения несанкционированным источником.

Список использованных источников:

1 Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICDN 100-101/ У. Одом – Вильямс, 2017. – 912 с.

2. Таненбаум, Э., Уэзеролл Д. Компьютерные сети : учеб. пособие / Э. Таненбаум, Д. Уэзеролл. – СПб.: Питер, 2013. – 960 с.

ОПТИМИЗАЦИЯ СТРУКТУРЫ ФИЛЬТРОВ-ДЕЦИМАТОРОВ С ПОМОЩЬЮ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

Костенок П.Д, Арлович С.В., Козел Д.И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Печень Т.М. – старший преподаватель

Рассматривается реализация КИХ фильтров и их преимущество, а также алгоритм работы фильтров. Предложена архитектура фильтра с коэффициентом децимации более 2 для случая блочных данных.

Цифровой фильтр-ресеплер с конечной импульсной характеристикой (КИХ) - это фильтр, импульсная характеристика которого или ответ на любой вход с конечной длиной, имеет конечную длительность, так как он оканчивается на ноль за конечное время. КИХ-фильтр может использоваться для реализации практически любого вида частотной характеристики в цифровом виде. [1].

При реализации КИХ-фильтров в программируемых логических интегральных схемах (ПЛИС), их возможности могут существенно ограничиваться некоторыми ресурсами ПЛИС. Наиболее «дефицитным» обычно оказывается такой ресурс как умножители (англ. multiplier's).

Из-за нехватки умножителей разработчикам приходиться применять более дорогостоящие ПЛИС, снижать порядок фильтра, уменьшать их количество доступных номиналов цифровых полос, что в итоге негативно сказывается на технических характеристиках конечного продукта.

Для оптимизации структуры КИХ-дециматоров необходимо выполнить следующие итераций:

– Вычислить соответствующие коэффициенты КИХ-фильтра и порядка цифрового фильтра.

Характеристика классического КИХ фильтра может быть представлена в виде:

$$y(n) = \sum_{i=0}^{n} b_i x(n-\mathrm{i}) \tag{1}$$

где n-порядок фильтра,
bi – коэффициент фильтра.

Структурная схема нерекурсивного КИХ-фильтра показана на рисунке 1.

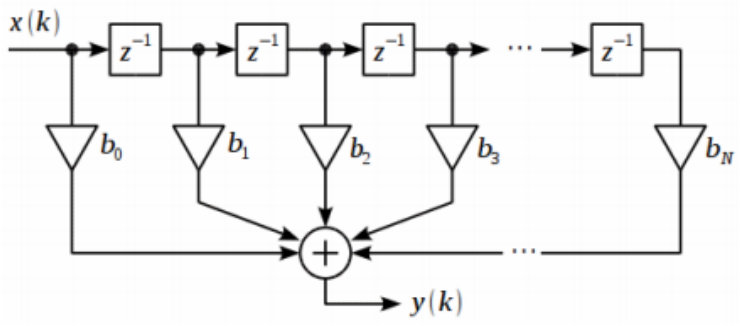


Рисунок 1 – Структурная схема нерекурсивного КИХ-фильтра

КИХ фильтр порядка n содержит n линий задержки и n+1 коэффициент. Если коэффициент b0 = 1, то получим КИХ фильтр порядка n, у которого умножение на b0 = 1 будет тривиальным.

Импульсная характеристика КИХ-фильтра всегда конечна и полностью совпадает с коэффициентами фильтра. Массив таких фильтров позволяет реализовать m различных номиналов цифровых полос, где m – любое целое число.

– Оценить потребность в ресурсах типа умножители для такого массива фильтров:

$$M = (n+1) \times m \tag{2}$$

– Рассмотреть в качестве альтернативного решения р архитектору буферного КИХ фильтра-дециматора, приведенную на рисунке 2.

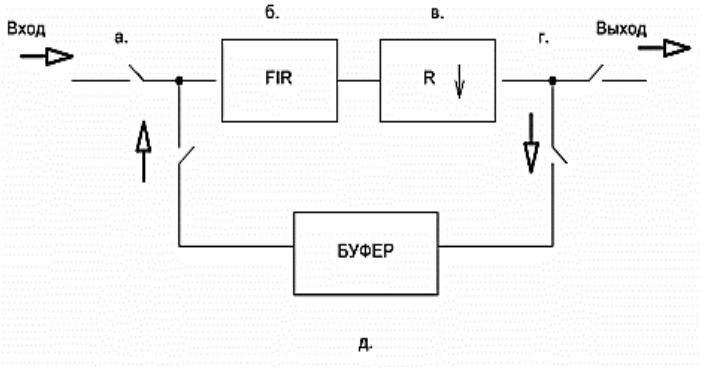


Рисунок 2 – Структурная схема буферного КИХ фильтра

где а – входной логический переключатель; б – полуполосный (halfband) КИХ фильтр; в – блок децимации с коэффициентом R=2; г – выходной логический переключатель; д – буфер.

Входными данными для такого фильтра могут быть отсчеты цифрового сигнала, предварительно преобразованного на 0 Гц.

– Оценить схему обработки данных таким фильтром.

1. Данные поступают во входной логический переключатель, а) рис.1. и перенаправляются на вход КИХ фильтра б), который предназначен, прежде всего, для устранения алиасинга во входном сигнале при децимации.

2. После фильтрации тактовая частота сигнала уменьшается вдвое с помощью дециматора в).

3. После децимации данные поступают в выходной коммутатор г). В случае, если необходимая полоса сигнала не достигнута, данные перенаправляются в буфер г).

4. После заполнения буфер возвращает блок данных через входной коммутатор а), для следующей итерации по сужению полосы.

5. Итерации 2-4 повторяются до достижения необходимой полосы сигнала. Очевидно, что для блочных данных, за счет циклической структуры обработки сигнала, можно реализовать на одном фильтре любые коэффициенты децимации кратные 2k, где k = 1, 2, 3, …

– Рассмотреть дополнительные возможности по оптимизации требований КИХ фильтра к количеству умножителей, необходимых для его реализации в современных программируемых логических интегральных схемах.

Для анализа необходимо ввести следующие ограничения в структуру фильтра: пусть каждый второй коэффициент фильтра равен нулю и коэффициенты фильтра симметричны относительно центрального коэффициента.

– Учесть при проектировании фильтра необходимым и достаточным условием равенства нулю каждого второго коэффициента является полуполосность фильтра, то есть симметричность значений частоты среза (Wpass) и частоты заграждения (Wstop), относительно половины частоты дискретизации (Fs/2) [2].

– При реализации буфера фильтра необходимо учитывать следующую важную особенность, что КИХ фильтр – это нерекурсивный фильтр или фильтр свертки. КИХ фильтры выполняют свертку своих коэффициентов с последовательностью входных отсчетов данных, при этом результирующий объем данных возрастает по формуле:

$$К = К_Д + К_Ф - 1 \quad (3)$$

где К — количество элементов в выходной последовательности;
КД — количество входных отсчетов данных;
КФ — количество коэффициентов фильтра.

При этом первые КФ — 1 отсчетов выходной последовательности не являются валидными.

Таким образом, у предложенной архитектуры существует некоторые ограничения на применение, а именно: фильтр может эффективно применяться с коэффициентом децимации более 2 только с блочными данными; коэффициенты децимации могут быть только числами кратными 2k; фильтр имеет относительно «жесткую» структуру, а именно, равенство нулю каждого второго коэффициента и симметричность коэффициентов относительно центрального коэффициента.

Список использованных источников:

1. Карбушов, Ч.С. Разработка КИХ-фильтра с использованием распределенной арифметической архитектуры // Технические науки: проблемы и перспективы: материалы V Международной научной конференции. – 2017.

2. Steven W. Smith, The Scientist and Engineer's Guideto Digital Signal Processing, Second Edition, 1999, California Technical Publishing, P.O. Box 502407, San Diego, CA 92150.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ДОМОМ SMART HOME

Лазоркин И.О.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Давыдова Н.С. – канд. тех. наук, доцент

«Smart Home» – это система, позволяющая связать воедино набор электронных устройств независимо от производителя и автоматизировать бытовые процессы в доме через единый центр управления, в котором будет осуществляться конфигурация и мониторинг каждого из устройств. Так же её неотъемлемой частью является возможность создания сценариев совместной работы таких устройств исходя из требований конкретного пользователя.

Как правило «умный дом» состоит из следующих компонентов:

– программное обеспечение;
– контроллеры;
– оборудование автоматизации;
– исполнительные устройства;
– датчики;
– устройства управления.

Функции и возможности, предоставляемые подобными системами можно объединить в следующие категории:

– безопасность;
– комфорт;
– экономия и защита окружающей среды;
– здоровье;
– автоматизация и автономность;
– удаленный доступ.

Безопасность.

Данная категория включает в себя функции видеонаблюдения, имитации присутствия, контроля и управления доступом, охранной и пожарной сигнализации.

Например, если при отсутствии владельцев в доме датчик движения зарегистрировал некую активность, об этом информируется охранная организация, а на смартфон приходит оповещение в виде SMS-сообщения или PUSH-уведомления с выводом изображения с камер видеонаблюдения.

Помимо контроля и управления доступом часть радиочастотных меток может использоваться системой автоматизации для запуска определенных сценариев.

Комфорт.

Данная категория включает в себя функции управления освещением, температурой и медиа-центром, взаимодействие с системой с помощью голоса и мобильных устройств.

Как правило управление любым из подключенных к системе устройств, может осуществляться при помощи браузера, специального приложения или голосовых команд не зависимо от операционной системы и модели устройства.

Так же голосовой помощник может реагировать на огромное количество команд, будь то запрос информации о погоде или пробках, вплоть до бронирования столика в ресторане.

Экономия и защита окружающей среды.

Данная категория включает в себя функции контроля энергопотребления устройств, газо- и водоснабжения.

Например, при наличии двухтарифного счетчика электроэнергии и договора с электроснабжающей компанией можно сократить расходы на электроэнергию, используя функции отложенного запуска энергоёмких устройств в льготные часы.

Еще одним примером может служить установка солнечных панелей на крышу своего жилища. Аккумулируя полученную с их помощью энергию и используя её в часы максимальной

стоимости, можно не только хорошо сэкономить, но и снизить вред, наносимый окружающей среде, за счет использования возобновляемого источника энергии.

Здоровье.

Данная категория включает в себя функции контроля качества воды и воздуха.

Система автоматизации может осуществлять мониторинг состояния воздуха и определить в какой момент необходимо проветрить помещение или начать процедуру очистки, а также в случае обнаружение посторонних газов сообщит об этом.

В свою очередь наблюдение за химическим составом воды позволит определить эффективность и ресурс очищающего фильтра, а также проинформирует владельцев о необходимости его замены.

Автоматизация и автономность.

Данная категория включает в себя функции настройки оборудования и создания сценариев поведения системы исходя из потребностей пользователя или в случае отказа одного из устройств.

Легкость настройки и замены каждого из устройств является одной из приоритетных задач систем домашней автоматизации, а резервирование ключевых элементов и источников питания обеспечит функционирование системы при чрезвычайных ситуациях.

В свою очередь использование сценариев позволяет расширить функционал системы и создать более гибкую конфигурацию.

Удаленный доступ.

Данная категория включает в себя функции мониторинга и удаленного управления системой автоматизации.

Удаленный доступ к системе позволит в любой момент проверить состояние жилища и вручную инициализировать запуск любого из сценариев, результат выполнения которых будет передан и обработан центром управления.

ПРОЦЕДУРА ИНТЕРЛИВИНГА В СИСТЕМАХ DWDM С КОГЕРЕНТНЫМ ПРИЕМОМ СИГНАЛОВ

Латушкин К.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Урядов В.Н. – к.т.н.,доцент

В данной работе рассматривается возможность упрощенной реализации процедуры демультиплексирования в системах DWDM, что позволяет говорить об экономической выгоде от внедрения данного метода. Вместе с тем проводится оценка выигрыша связанного с избавлением от процедуры интерливинга.

Устройство интерливинга разделяет каналы, которые подлежат мультиплексированию, на группы: нечетные и четные для конфигурации интерливинга 1×2. В этом простейшем случае устройство интерливинга объединяет два набора каналов в один плотно упакованный набор, имеющий шаг упаковки в два раза меньше исходного. В противоположность этому, устройство деинтерливинга разделяет единый входной набор каналов и направляет разделенные потоки в два выходных потока, имеющих удвоенный шаг между каналами по сравнению с исходным [1]. Пояснения к процедуре интерливинга приведены на рисунке 1.

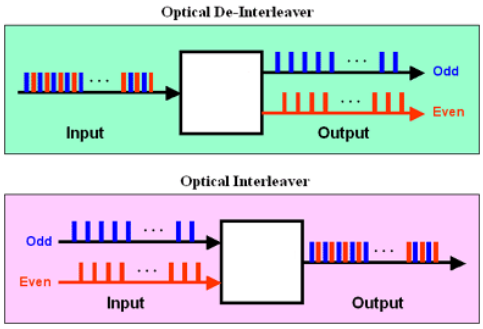


Рисунок 1 – Процедура интерливинга

Применение когерентного детектирования, даже по сравнению с оптическими усилителями EDFA имеет существенные преимущества с точки зрения чувствительности приемника. Гетеродинный метод приема не требует согласования фаз оптических полей. Но требуется поддерживать постоянство разности между частотой входного информационного оптического сигнала и частотой местного гетеродина для компенсации уходов и нестабильности частоты входного сигнала, возникающих по причине температурной нестабильности и других внешних факторов. Для обеспечения постоянства разности частот производят подстройку частоты местного гетеродина при помощи контроллера частоты.

Для этого в спектр информационного сигнала перед модуляцией оптической несущей вводится однотональный сигнал с амплитудой A и частотой $f_д$, превышающей верхнюю частоту информационного сигнала. В результате модуляции в спектре информационного сигнала помимо информационных составляющих появятся две дополнительные составляющие с частотами $f_c \pm f_д$. В волокне со стороны приемника при помощи распределенного усилителя Бриллюэна производится избирательное усиление частоты $f_c + f_д$. Далее сформированный таким образом сигнал подается на вход фотодетектора. Данный приемный оптический модуль функционирует по принципу гетеродинного приемника, а в качестве сигнала местного гетеродина используется усиленная составляющая с частотой $f_c + f_д$. Высокий коэффициент усиления распределенного усилителя Бриллюэна позволяет получить существенное увеличение ее мощности. На выходе фотодетектора будет получен информационный сигнал на поднесущей частоте $f_д=f_п$ [2].

Таким образом, используя метод гетеродинного приема с использованием распределенных усилителей Бриллюэна, а также принимая во внимание, что разнос частот между каналами в системах DWDM является постоянным, появляется возможность используя усиленную частоту $f_c + f_д$ четного канала, как опорную и для нечетного и для четного каналов, таким образом нет необходимости в процедуре деинтерливинга

Список использованных источников:

1. Иванов,В.И. Применение технологии WDM в современных сетях передачи информации: учеб. пособие / В.И. Иванов. – Казань:ПГУТИ, 2010. – 148 с.

2. Урядов, В.Н. Трансформация спектра оптического сигнала при реализации гетеродинного приема в ВОСП / В.Н. Урядов [и др.] // Электросвязь. – 2018. – №9. – С. 61-65.

МЕТОДИКА ОЦЕНИВАНИЯ ШУМА КВАНТОВАНИЯ ЦИФРОВОГО ФИЛЬТРА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь,

Левчук В.А., Подинако А.В., Арлович С.В.

Печень Т.М. – Старший преподаватель

Предложена методика оценивания шума квантования цифрового фильтра. В данной работе изучены такие характеристики цифрового фильтра, как шум квантования, отклик фильтра на входной шум, ошибка сигнала в любой точке структуры фильтра, дисперсия входного шума, дисперсия шума квантования на выходе фильтра.

Методика оценивания шума квантования цифрового фильтра предусматривает следующие этапы:

– Если на вход цифрового фильтра с импульсной характеристикой h(t) поступает сигнал x(t), то выходной сигнал фильтра определяется выражением:

$$y(n) = \sum_{m=0}^{N-1} h(m)x(n-m)$$

В результате квантования входного сигнала образуется шум квантования $e_{in}(n)$, который накладывается на входной сигнал и воздействует на фильтр. В силу линейности фильтра можно вычислить реакцию фильтра $e_{out}(n)$ на входной шум. При этом подразумевается, что все вычислительные устройства и запоминающие устройства, используемые при конструировании фильтра имеют бесконечную разрядность.

– Для нахождения ошибки сигнала в любой точке структурной схемы фильтра, обусловленную шумом квантования входного сигнала $e_{in}(n)$ необходимо воспользоваться формулой:

$$e_i(n) = \sum_{m=0}^{N-1} h_i(m)e_{in}(n-m)$$

где $h_i(n)$ – импульсная характеристика части фильтра от его входа до точки, в которой оценивается ошибка.

Если входной сигнал фильтра квантуется с разрядностью b_{in}, то ошибка квантования входного сигнала при использовании округления ограничена величиной описанной в следующим выражением:

$$E_{in} = \max(|e_{in}(n)|) = 2^{-b_{in}-1} = \frac{Q_{in}}{2}$$

А ошибка выходного сигнала фильтра, вызванная квантованием входного сигнала может быть оценена как [1]:

$$E_{out} = \max(|e_{out}(n)|) \le \max(|e_{out}(n)|)\sum_{m=0}^{\infty}|h(m)| \le \frac{Q_{in}}{2}\sum_{m=0}^{\infty}|h(m)|$$

Таким образом, верхняя граница ошибки, вызванной квантованием входного сигнала, зависит от разрядности квантования и от суммы модулей выборок импульсной характеристики фильтра.

Согласно равенству Парсеваля дисперсию можно определить следующим выражением:

$$\sigma^2_{out} = \sigma^2_{in}\frac{T}{\pi}\int_0^{\pi/T}\left|H(e^{j\omega T})\right|^2 d\omega$$

где $|H(e^{j\omega T})|$ - АЧХ цифрового фильтра.

Таким образом, по допустимой величине s_{out}^2 и известной АЧХ или ИХ фильтра можно определить допустимую величину дисперсии ошибки входного сигнала s_{in}^2, которая в свою очередь определяет требуемую разрядность b_{in} квантования входного сигнала.

Список использованных источников:

1. Витязев, В.В. Многоскоростная адаптивная обработка сигналов // Радиотехника. – 2012. – № 3. – С. 17–29.
2. Витязев, В.В. Многоскоростная обработка сигналов в системах телекоммуникаций // Электросвязь. –2013. – № 11. – С. 49–56.

ИССЛЕДОВАНИЕ БИХ-ФИЛЬТРОВ В СРЕДЕ SIMULINK

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Лешкевич М.Н., Подинако А.В, Сугако А.В.

Печень Т.М. – Старший преподаватель

В данной работе рассмотрена математическая модель дискретного фильтра с бесконечной импульсной характеристикой. Для исследований выбрана математическая среда Simulink.

Интегрирование, как математическая операция, занимает важное место в системах обработки сигналов. Варианты КИХ-интегратора и быстрой свертки отпадают, если иметь в виду качество выполнения операции. Остается вариант БИХ-интегратора. Замена непрерывного времени на дискретное дает [1]:

$$g(n) = \begin{cases} 0{,}5\,, & n = 0 \\ 1\,, & n > 0 \end{cases} \quad (1).$$

Системная функция для дискретного интегратора с данной ИХ равна:

$$D(z) = \sum_{n=0}^{\infty} z^{-n} - 0{,}5 = 0{,}5 \times \frac{1+z^{-1}}{1-z^{-1}} \quad (2).$$

Работа данной функции реализована в SIMULINK и показана на рисунке 1:

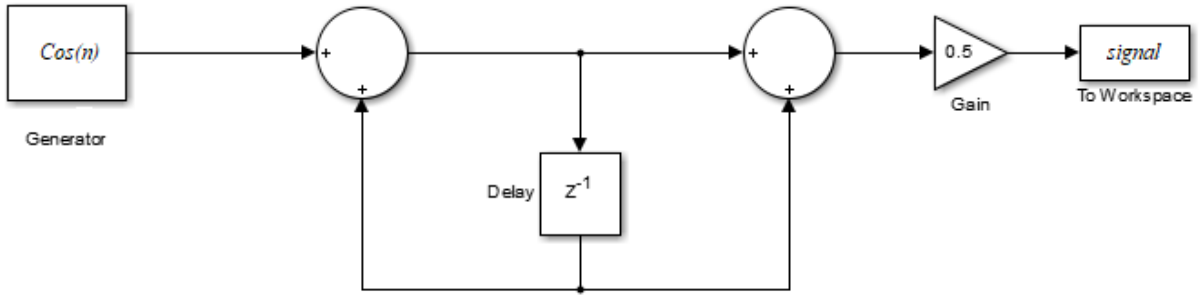


Рисунок 1 – Схема интегратора, использующего каноническую форму, которая позволяет обойтись одним регистром сдвига

Схема генератора, представленного на рисунке 1:

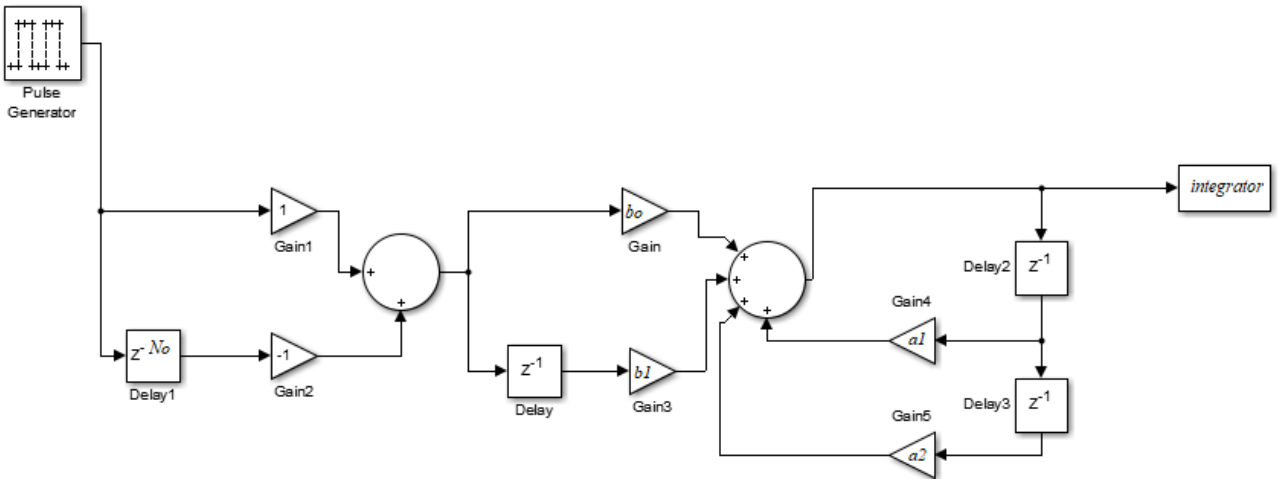


Рисунок 2 – Схема образования косинусоидального сигнала.

Рассмотреть сигнал, выходящий из генератора косинусоидальных импульсов, имеем возможность на рисунке 3.

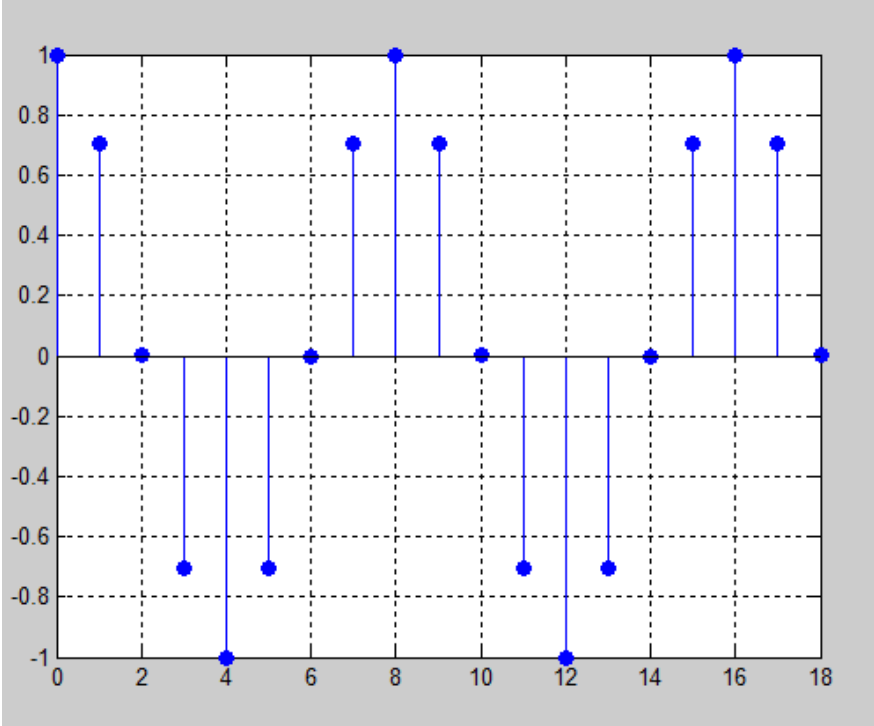


Рисунок 3 – Вид сигнала, выходящего из генератора на рисунке 2

Начальная фаза сигнала выбрана таким образом, чтобы косинусоидальные импульсы начинали поступать от начала системы отсчета.

Далее этот сигнал поступает на вход генератора и преобразуется согласно системной функции. Преобразование сигнала в интеграторе, имеем возможность рассмотреть на рисунке 4:

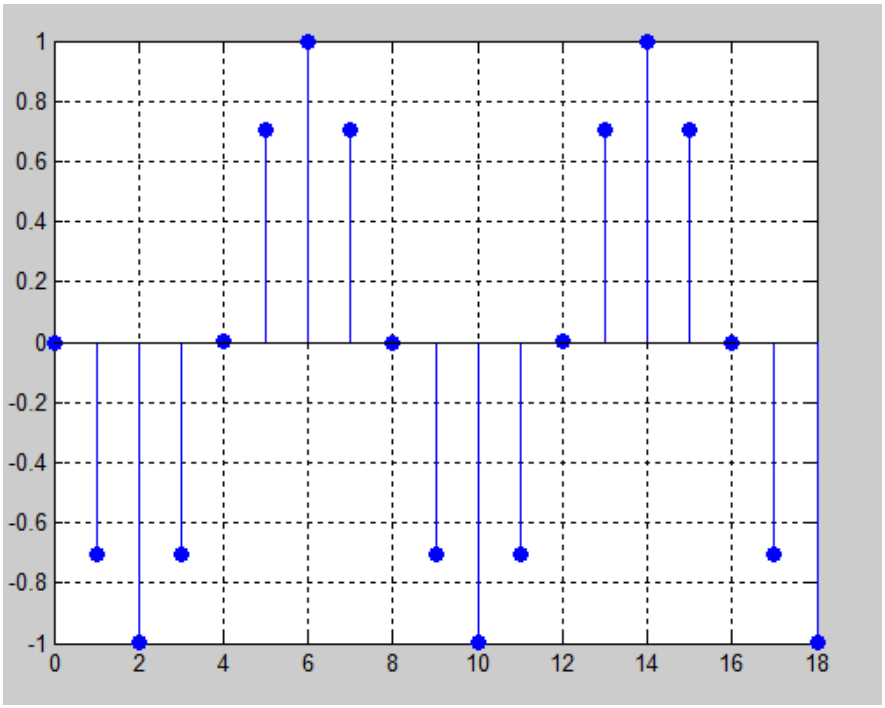


Рисунок 4 – Вид сигнала на выходе генератора, после преобразований

Таким образом, можно сделать вывод, что схема работает исправно: первообразный интеграл от функции синуса сохраняется. Простейшим БИХ-фильтром является дискретный интегратор.

Список использованных источников:
1. Овсянников, В. А. Методы формирования и цифровой обработки сигналов : учебно-метод. пособие : в 2 ч. Ч. 2 : Дискретное преобразование Фурье, фильтрация и модуляция / В. А. Овсянников. - Мн. : БГУИР, 2010.

ОБРАБОТКА ЦИФРОВЫХ АСМ-ИЗОБРАЖЕНИЙ НА ОСНОВЕ ГЕОМЕТРИЧЕСКИХ ПАРАМЕТРОВ ТОПОГРАФИЧЕСКИХ ЭЛЕМЕНТОВ ПОВЕРХНОСТЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ловецкий М.Ю.

Астровский И.И. – к.т.н., доцент

В представленной работе проведена оценка эффективности алгоритмов и программных средств сегментации, обеспечивающих выделение областей изображений атомно-силовой микроскопии, соответствующих элементам поверхностей неорганических материалов. Также разработаны: алгоритм параметризации и разбиения топографического пространства на симплексы, учитывающий особенности изображений атомно-силовой микроскопии, обеспечивающий описание материалов; алгоритм фильтрации АСМ-изображений на основе форм-факторов сегментов; алгоритм высокоточной совмещения и сшивки цифровых изображений атомно-силовой микроскопии неорганических материалов с использованием геометрических параметров топографических элементов поверхностей.

В качестве исходных данных используются результаты сканирования поверхности одного образца неорганического материала в разных участках, представленные на рисунке 1.

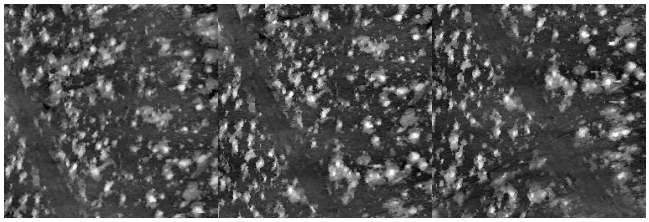


Рисунок 1 – Образец поверхности с напылением алюминия, отсканированный в различных участках

Изображения проходят предобработку в виде применения фильтра Гаусса с размером окна 10, затем алгоритмом ВОЛМА на изображениях выделяются сегменты. На основе найденных областей определяются опорные точки изображения и их ближайшие соседи, на основе которых составляются дескрипторы точек. Данные дескрипторы сравниваются для всех пар совмещаемых изображений. Для каждой пары точек, идентифицированных на двух совмещаемых изображениях, находится разность оси ординат и абсцисс. Определяется набольшее значение вероятности разности координат для всех совмещаемых точек. Данное значение принимается за величину смещения, после чего происходит совмещение двух изображений со смещением. Сшитое изображение представлено на рисунке 2.

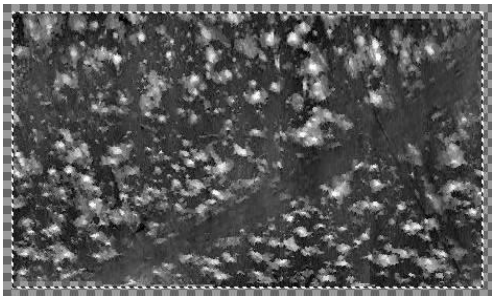


Рисунок 2 – Результат сшивки трех сканированных участков одного образца

Как видно из полученных данных разработанный алгоритм позволяет произвести высокоточную сшивку АСМ-изображений, на основе найденных особых точек. Дефект напыления заметный на трех образцах прослеживается на результирующей матрице. Полученные результаты в дальнейшем можно развить для автоматического выделения объектов, с заданными параметрами, классификацию найденных объектов, их параметризацию и идентификацию в базе

данных, либо на нескольких образцах. Так же разработанные алгоритмы можно модифицировать для анализа получаемых данных.

Список использованных источников:

1. Eaton, P. Atomic Force Microscopy / P. Eaton, P. West. – Oxford Univ. Press, 2010. – 257 p.

2. Рабцевич, В. В. Регрессивный алгоритм сегментации АСМ-изображений на основе волнового выращивания областей / В. В. Рабцевич, В. Ю. Цветков, Ловецкий М. Ю. // Мониторинг техногенных и природных объектов: сб. материалов междунар. научн. -техн. конф. / редкол. : Батура М. П. [и др.]. – Минск: БГУИР, 2017. – С. 77 – 84.

ИССЛЕДОВАНИЕ ДИФФЕРЕНЦИРОВАНИЯ СИГНАЛОВ В СРЕДЕ SIMULINK

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Максимович В.С., Дулуб И.В.

Печень Т.М. – Старший преподаватель

В данной работе рассмотрена математическая модель дискретного дифференциатора в виде фильтра с конечной импульсной характеристикой. Исследования проведены в математической среде Simulink.

Развитие средств современной микропроцессорной техники и снижение их стоимости открывают широкие возможности для совершенствования уже имеющихся и создания новых алгоритмов решения в реальном масштабе времени многих прикладных задач. Одной из таких задач является рассматриваемая в данной работе задача цифрового дифференцирования сигналов (ЦДС), измеряемых в реальном масштабе времени в системах автоматического регулирования [1].

$$g(n) = \frac{2\mathrm{F}f_{\mathrm{д}}}{n-\alpha}\left[\cos 2\pi\theta(n-\alpha) - \mathrm{Sinc}\left(2\pi\theta(n-\alpha)\right)\right], \quad \textbf{(1)}$$

где $\alpha = \frac{T}{\Delta t} = Tf_{\mathrm{д}} = \frac{N-1}{2}$; $\theta = \frac{F}{f_{\mathrm{д}}}$, n=0(1)N-1.

Ниже приведена структурная схема реализации дифференцирования сигналов (рис.1).

Рисунок 1 - Структурная схема исследования дифференцирования сигналов

На основании структурной схемы была разработана функциональная схема системы для моделирования в среде Simulink (рис. 2).

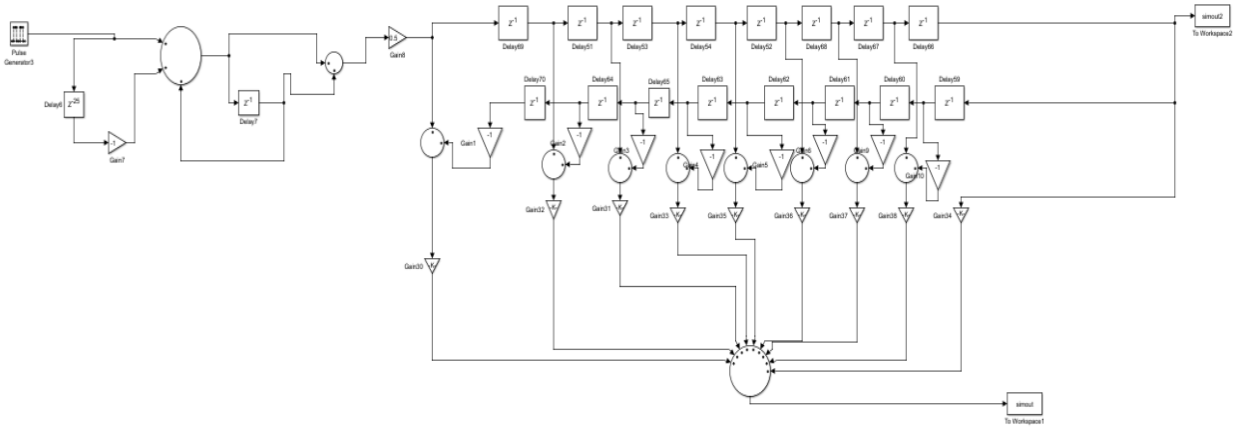


Рисунок 2 - Схема моделирования в Simulink

Данная схема со средней точкой выдает сигнал и его производную в совпадающие моменты времени. На рисунке 3 представлен график входного сигнала на выходе средней точки.

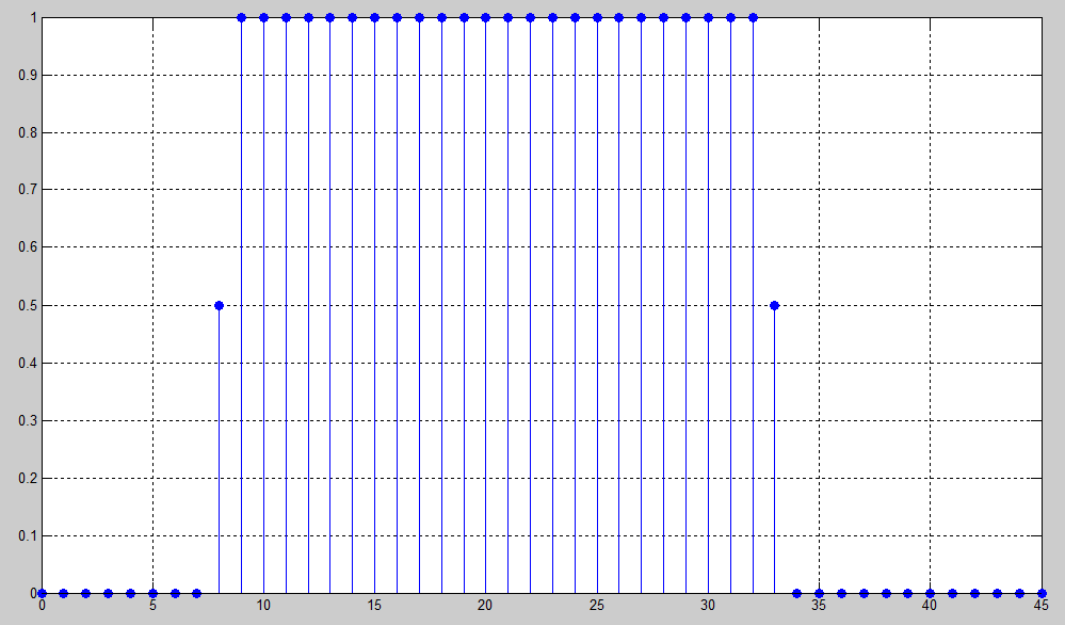


Рисунок 3 - График сигнала на выходе средней точки схемы исследования в Simulink

Схемы со средней точки предпочтительнее для использования, т.к. все преобразования являются инерционными, то для анализа реакции системы на выходе именно график на рис. 4 сравнивается с рис. 3.

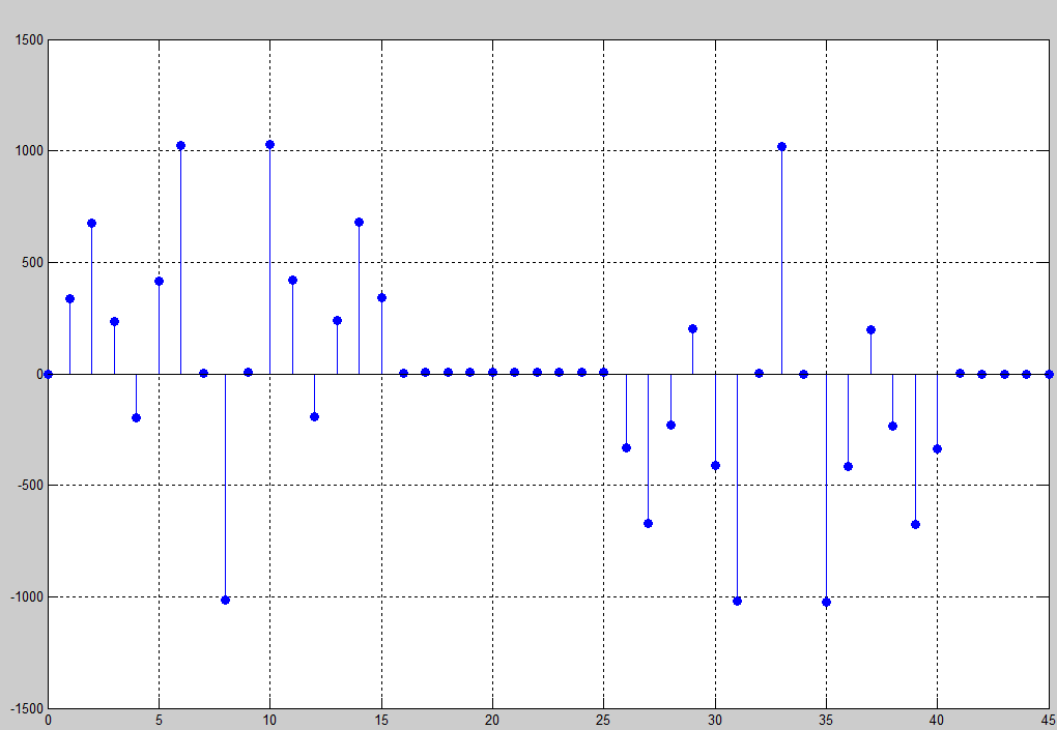


Рисунок 4 - Сигнал на выходе

Таким образом, можно сделать вывод, что при моделировании цифровых или дискретных систем необходимо обязательно учитывать шаг дискретизации, выбор количества отсчётов импульсной характеристики, параметры входного сигнала, т.к. именно от этого зависит качество работы устройств [2]. Сигнал на выходе исследуемой в данной работе системы имеет искажённый вид и побочные компоненты. Это обусловлено выбором небольшого количество отсчётов ИХ

дифференциатора и более протяжённым сигналом на входе устройства. Точно фильтрации напрямую зависит от согласования параметров и характеристик устройств системы.

Список использованных источников:

1.Овсянников В.А. Методы формирования и цифровой обработки сигналов. Часть 1. Z-преобразование, свертка и генерация дискретных сигналов- Минск 2007.

2.Першин В.Т. Формирование и генерирование сигналов цифровой радиосвязи : учеб.-метод. Пособие. В 2 ч. Ч.1. – Минск: БГУИР

МОДЕЛИРОВАНИЕ ВЫСОКОЧАСТОТНЫХ КОЛЕБАНИЙ С ПОМОЩЬЮ АЛГОРИТМОВ БПФ-ОБПФ

Педченко Н.В., Король А.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Печень Т.М. – старший преподаватель

В данной работе приведены результаты моделирования высокочастотных колебаний в специализированной программе “Фурье анализ и синтез”. Исследования проводились на основании алгоритмов прямого и обратного быстрого преобразования Фурье.

В задачах модуляции и демодуляции широко применяются алгоритмы БПФ-ОБПФ. На кафедре инфокоммуникационных технологий для проведения лабораторных работ была разработана специализированная программа “Фурье анализ и синтез”. В данной работе рассмотрим случай создания радиоимпульса по схеме представленной на рисунке 1.

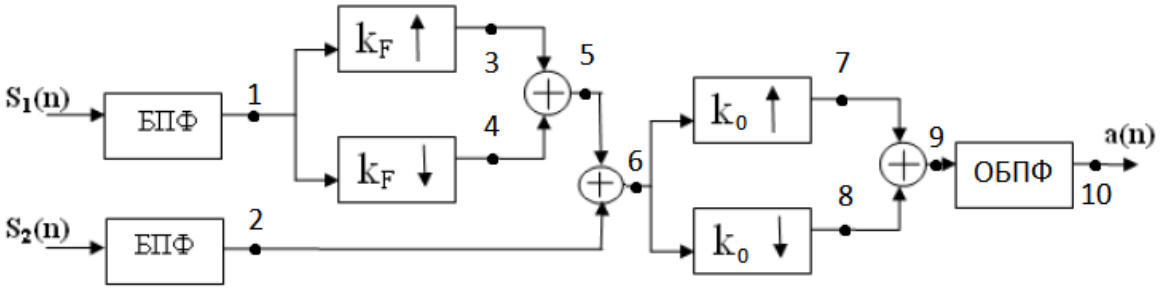


Рисунок 1 – Схема формирования радиоимпульса

СКО=15
A=5
$N_{S1} = 121$

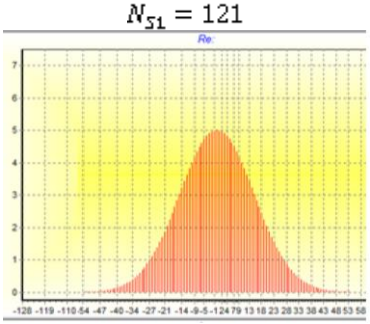


Рисунок 2 – Входной колокольный сигнал $S_1(n)$

СКО=31
A=5
$N_{S2} = 151$

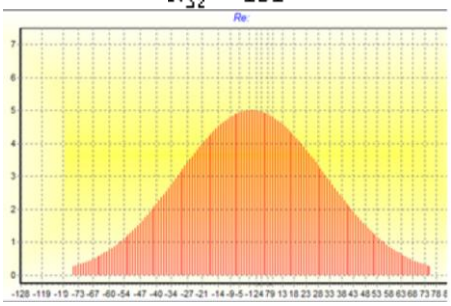


Рисунок 3 – Входной колокольный сигнал $S_2(n)$

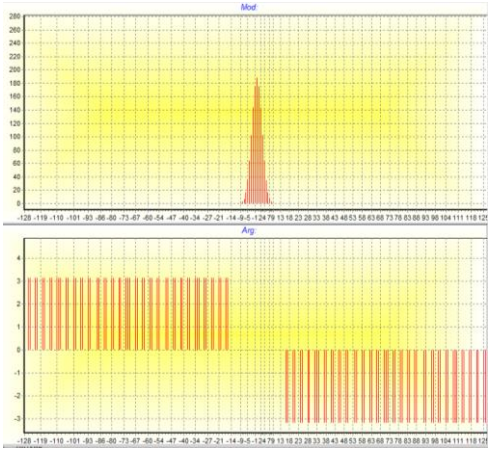


Рисунок 4 – Спектр сигнала в точке 1

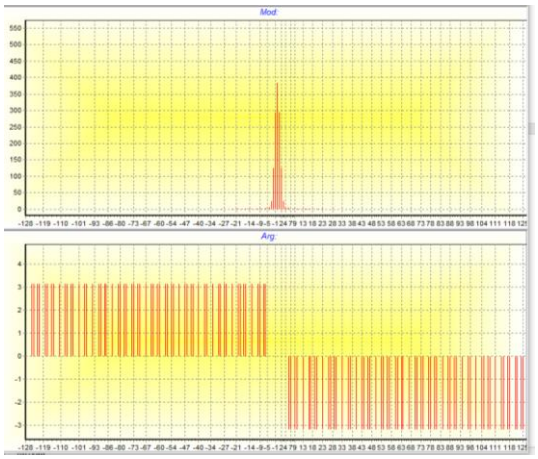


Рисунок 5 – Спектр сигнала в точке 2

В точке 3 сдвинули спектр вправо на частоту модулирующего колебания $K_F = 33$, в точке 4 влево на $K_F = -33$.

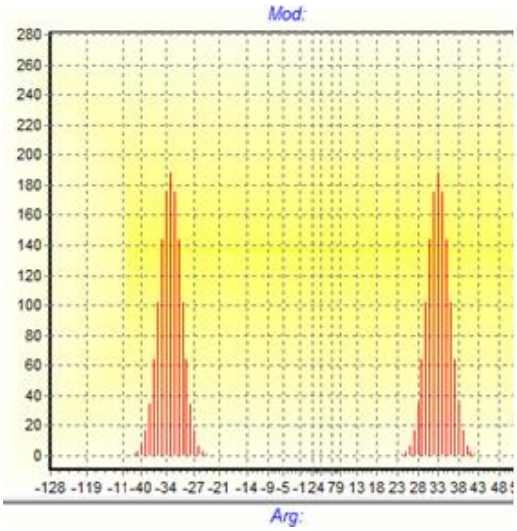


Рисунок 6 – Сумма сдвинутых спектров сигнала $S_1(n)$

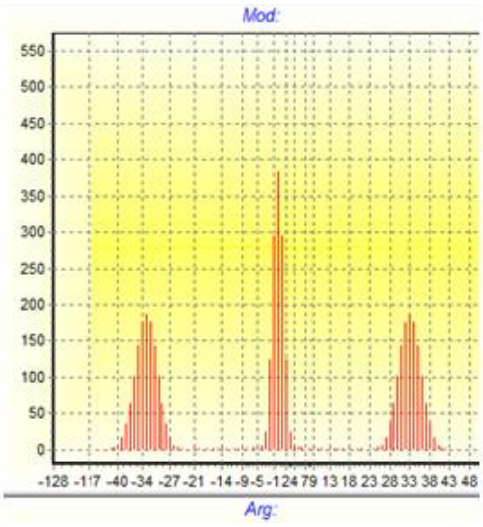


Рисунок 7 – Сумма спектра сигнала $S_2(n)$ и сдвинутых спектров сигнала $S_1(n)$

В точке 5 сдвинули спектр вправо на частоту несущего колебания $K_D = 107$, в точке 6 влево на $K_D = -107$.

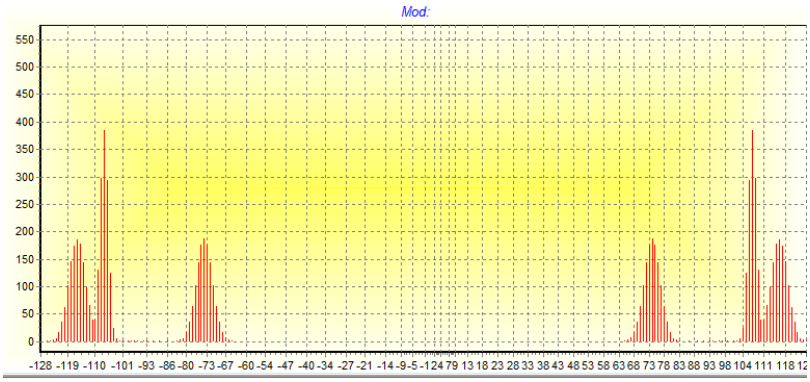


Рисунок 8 – Сумма сдвинутых спектров в точке 7

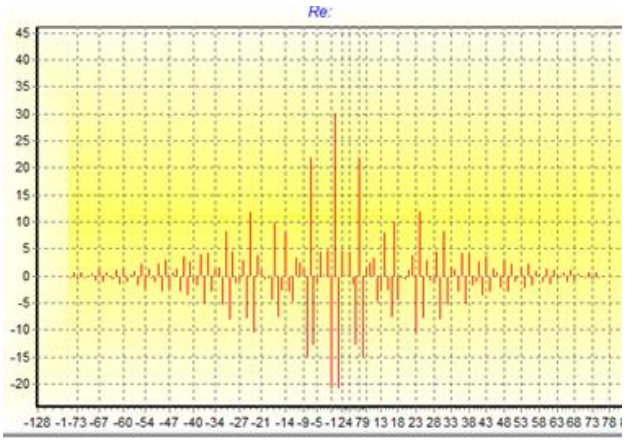


Рисунок 9 – Результат в точке 10 после ОБПФ

Вывод: алгоритмы БПФ-ОБПФ позволяют эффективно моделировать процесс генерации сложных высокочастотных колебаний для передачи по каналам связи.

Список использованных источников:

1. Овсянников В.А. Методы формирования и цифровой обработки сигналов. Часть 2. Дискретное преобразование Фурье, фильтрация и модуляция- Минск 2007.

ЗАЩИТА ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ ОТ ИНФОРМАЦИОННЫХ АТАК

Полещук В.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ширинский В.П. – к.т.н.,доцент

Изложены причины возникновения информационных атак, их сущность и стадии развития (жизненный цикл). Дается обзор средств обнаружения и предотвращения атак, принципы действия данных систем и перспективы развития.

Уровень криминогенности в информационной сфере сетей передачи данных ведущих стран мира постоянно повышается, несмотря на интенсивное внедрение вновь создаваемых технологических решений в области информационной безопасности. Это приводит к миллиардным финансовым потерям в глобальном масштабе. Проблема усугубляется также постоянным ростом уровня сложности информационных атак.

В свете вышеизложенного, защита ИКС от информационных атак является одной из наиболее актуальных и значимых задач в области индустрии интернет-технологий (ИТ-индустрии).

Практически любая автоматизированная система может выступать в качестве объекта информационной атаки, которая может быть определена как совокупность действий злоумышленника, направленная на нарушение одного из трех свойств информации — конфиденциальности, целостности или доступности.

Основной причиной возникновения информационных атак являются уязвимости. Наличие самих слабых мест в ИКС может быть обусловлено самыми различными факторами, начиная с простой халатности сотрудников и заканчивая преднамеренными действиями злоумышленников.

Уязвимости могут присутствовать как в программно-аппаратном, так и в организационно-правовом обеспечении ИКС.

Уязвимости программно-аппаратного обеспечения могут присутствовать в программных или аппаратных компонентах рабочих станций пользователей ИКС, серверов, а также коммуникационного оборудования и каналов связи ИКС. В соответствии с трехуровневой моделью узла ИКС, уязвимость может быть отнесена к аппаратному обеспечению, а также к общесистемному или прикладному ПО. В том случае, если уязвимость содержится в программно-аппаратном обеспечении ИКС, которое отвечает за организацию сетевого взаимодействия между узлами ИКС, она может быть дополнительно соотнесена с одним из пяти уровней модели ВОС - физическим, канальным, сетевым, транспортным или прикладным.

В отдельных случаях ошибки и недостатки могут содержаться не только в программно-аппаратном обеспечении ИКС, но и в спецификациях и стандартах, описывающих протоколы стека TCP/IP. В основном такие недостатки связаны с отсутствием в протоколах встроенных средств защиты, что делает их уязвимыми к различным информационным атакам.

Любая атака в общем случае может быть разделена на четыре стадии:

-Стадия рекогносцировки. На этом этапе нарушитель осуществляет сбор данных об объекте атаки, на основе которых планируются дальнейшие стадии атаки.Собираемая информации может включать тип и версию операционной системы (ОС), установленной на узлах ИКС, список пользователей, зарегистрированных в системе, сведения об используемом прикладном ПО и др

-Стадия вторжения в ИКС. На этом этапе нарушитель получает несанкционированный доступ к ресурсам тех узлов ИКС, по отношению к которым совершается атака.

-Стадия атакующего воздействия на ИКС. Данный этап направлен на достижение нарушителем тех целей, ради которых предпринималась атака. Примерами таких действий могут являться нарушение работоспособности ИКС, кража конфиденциальной информации, хранимой в системе, удаление или модификация данных системы и др. При этом атакующий может также осуществлять действия, которые могут быть направлены на удаление следов его присутствия в ИКС.

Стадия дальнейшего развития атаки. На этом этапе выполняются действия, которые направлены на продолжение атаки на ресурсы других узлов ИКС.

Изначально для обнаружения и отражения сетевых атак использовались межсетевые экраны (для блокирования сетевых соединений в процессе атаки) и разнообразное антивирусное ПО, срабатывающее, как правило, на 2-й и 3-ей стадиях. Однако данные средства показали свою ограниченную эффективность, что привело к появлению отдельных систем для обнаружения и отражения сетевых атак - IDS (intrusion detection system) и IPS (intrusion prevention system).

Задача IDS состоит в обнаружении и регистрации атак, а также оповещении при срабатывании определенного правила. В зависимости от типа, IDS умеют выявлять различные виды сетевых атак, обнаруживать попытки неавторизованного доступа или повышения привилегий, появление

вредоносного ПО, отслеживать открытие нового порта и т. д. Однако, в отличие от межсетевого экрана, контролирующего только параметры сессии (IP, номер порта и состояние связей), IDS «заглядывает» внутрь пакета (до седьмого уровня OSI), анализируя передаваемые данные. Существует несколько видов систем обнаружения вторжений. Весьма популярны APIDS (Application protocol-based IDS), которые мониторят ограниченный список прикладных протоколов на предмет специфических атак. Типичными представителями этого класса являются PHPIDS, анализирующий запросы к PHP-приложениям, Mod_Security, защищающий веб-сервер (Apache), и GreenSQL-FW, блокирующий опасные SQL-команды.

Сетевые NIDS (Network Intrusion Detection System) более универсальны, что достигается благодаря технологии DPI (Deep Packet Inspection, глубокое инспектирование пакета). Они контролируют не одно конкретное приложение, а весь проходящий трафик, начиная с канального уровня.

Системы IDS предназначены только для сигнализации обо всех все подозрительных действиях. Чтобы заблокировать атакующий хост, системный администратор самостоятельно перенастраивает брандмауэр во время просмотра статистики. В таком случае, однако, о реагировании в реальном времени речи не идет. Именно поэтому в настоящее время появились IPS (Intrusion Prevention System, система предотвращения атак). Они основаны на IDS, но могут самостоятельно перестраивать пакетный фильтр или прерывать сеанс, (например, отсылая TCP сообщение RST по протоколу TCP). В зависимости от принципа работы, IPS может устанавливаться «в разрыв» или использовать зеркалирование трафика (SPAN), получаемого с нескольких сенсоров. Примерами таких систем являются IBM Security Network Intrusion Prevention System, McAfee Network Security Platform, Suricata и др.

Однако современный Интернет несет огромное количество угроз, поэтому узкоспециализированные системы уже не актуальны. В связи с этим необходимо использовать комплексное многофункциональное решение, включающее все компоненты защиты: файервол, IDS/IPS, антивирус, прокси-сервер, контентный фильтр и антиспам-фильтр. Такие устройства получили название UTM (Unified Threat Management, объединенный контроль угроз). В качестве примеров UTM можно привести Trend Micro Deep Security, Kerio Control и др.

Список использованных источников:

3. В. Сердюк. Новое в защите от взлома корпоративных сетей // Техносфера. М. 2007 С.11–63.

БЕЗОПАСНАЯ ПОРТАТИВНАЯ ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ С АЛГОРИТМОМ ШИФРОВАНИЯ RABBIT STREAM

Рубинштейн Р. Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Цветков В. Ю. – д. т. н., доцент

В работе рассмотрена безопасная портативная виртуальная частная сеть с алгоритмом шифрования Rabbit Stream и проблемы, связанные с обеспечением ее безопасности и конфиденциальности.

Мобильность сотрудников стала одним из основных требований корпораций в наше время. Сотрудники часто получают командировку в филиалы или клиентские компании, которые находятся внутри или за пределами своей страны. Компания может соединить компьютерную сеть в центральном офисе с ее филиалами, расположенными далеко от Интернета, но она также может предоставить сотрудникам полномочия для доступа к внутренней сети компании. Однако, при передаче информации через Интернет существуют потенциальные уязвимости, такие как: перехват, мониторинг, модификация или изменение информации неуполномоченными сторонами .

Решение, которое можно использовать для преодоления такой уязвимости, заключается в использовании виртуальной частной сети (VPN). Компания предпочитает использовать VPN, а не использовать выделенную линию или выделенный путь провайдера. Помимо большей рентабельности, VPN также обеспечивает функции безопасности, например, шифрование и аутентификация. VPN-туннель сформирован для защиты связи между объектами в системе. OpenVPN является одной из самых популярных платформ VPN с открытым исходным кодом, разработанной Джеймсом Йонаном в 2002 году, и до сих пор продолжает разрабатываться сообществом разработчиков со всего мира.

Что касается платформы поддержки, OpenVPN уже может использоваться на многих платформах, например Операционная система на основе Linux, Debian, BSD, Microsoft Windows, Mac OS X и Solaris 4.

Существует два вида реализации VPN, то есть программная VPN и аппаратная VPN. Программная VPN является наиболее распространенной реализацией VPN. Он может быть установлен поверх операционной системы, поэтому пользователь может осуществлять удаленный доступ через свой ноутбук. Слабость этого типа реализации VPN заключается в том, что он потребляет память или ресурсы ЦП пользовательского ПК во время удаленного доступа. Поэтому производительность пользовательского ПК может быть ниже во время операции удаленного доступа. С другой стороны, в аппаратной VPN, отдельное оборудование используется для работы удаленного доступа. Аппаратная VPN имеет несколько преимуществ. Во-первых, его можно использовать в разных операционных системах ПК пользователя (независимо от платформы). Во-вторых, он более надежен, поскольку построен на отдельном оборудовании от ПК пользователя. В-третьих, у него также есть дополнительные функции, такие как встроенный брандмауэр и интернет-маршрутизация. В последнее время raspberry pi стала решением для ПК с низким энергопотреблением для любых приложений. Некоторые исследования были проведены для разработки аппаратного VPN на Rasberry Pi7,8.

В этом исследовании автор предлагает аппаратный прототип шлюза VPN, который работает на модели OSI уровня 4 (SSL VPN). SSL VPN выбран из-за фактора гибкости или простоты конфигурации, совместимости с трансляцией сетевых адресов (NAT) и отсутствия проблемы с правилами. Аппаратное обеспечение, используемое в предлагаемой системе, - SBC Raspberry Pi 3 Model B + с основными приложениями, которые модифицированы с помощью OpenVPN. Вдобавок к OpenVPN, алгоритм поточных шифров Rabbit реализован как альтернативный вариант шифровальных пакетов TLS. Алгоритм потоковых шифров Rabbit выбран из-за его криптографической стойкости и простых операций 10. Этот алгоритм также был стандартизирован IETF RFC 4503. По результатам тестирования и анализа этот алгоритм доказал свою эффективность в качестве криптографических и устойчивых криптографических аналитических методов.

Исследование состоит из нескольких этапов. Во-первых, мы выявили проблему с традиционным программным обеспечением VPN, как описано во введении. Во-вторых, мы проводим обзор литературы, чтобы найти современное состояние развития технологии VPN, как программного, так и аппаратного решения. В-третьих, мы предъявляем требования к проектированию и планируем разработку аппаратного и программного обеспечения. Наконец, мы выполняем оценку разработанного прототипа. В остальной части этой статьи обсуждается процесс проектирования и оценки прототипа.

Прототип предназначен для поддержки командировочных сотрудников для выполнения удаленного доступа к внутренней сети компании. Мы называем прототип AR-6000. На рисунке 1 показан сценарий использования AR-6000. Из рисунка 1 видно, что в системе зон AR-6000 есть два основных объекта:

• Пользовательская зона путешественника. Это зона, в которой находится деловой путешественник, который выполняет удаленный доступ пользователя. В этой зоне требуются следующие устройства: ПК или ноутбук, AR-6000 и точка доступа WLAN.

• Зона внутренних ресурсов: это местоположение сети внутренних ресурсов, где расположены серверы и компьютеры компании.

Пользователь берет с собой ноутбук AR-6000 во время командировки. AR-6000 действует как VPN-клиент. В случае, если он хочет получить доступ к внутренней сети, AR-6000 сформирует туннель для VPN-сервера. Он применяет SSL VPN для защищенных данных транзакций из внутренних сетей и через них. Затем пользователь может получить удаленный доступ к внутренней сети компании, чтобы продолжить свою работу на сервере. Есть несколько причин, по которым мы превращаем VPN-клиента в отдельное оборудование. Этот прототип предназначен для выполнения следующих требований:

• Прототип должен быть удобным для пользователя, что означает, что он может быть легко использован любым пользователем без необходимости выполнять настройку каждый раз, когда он хочет его использовать.

• Прототип необходим для работы на всех платформах. Это означает, что прототип можно использовать со всеми типами клиентских операционных систем (ОС) с помощью интернет-соединения.

• Если устройство нуждается в реконфигурации, мы можем настроить его, подключившись к устройству через безопасное соединение оболочки (SSH).

• Требуется, чтобы устройство было способно защищать передачу данных от VPN-клиента к VPN-серверу.

Каждый раз, когда пользователь выполняет удаленный доступ к внутренним ресурсам, AR-6000 получает запрос от ПК пользователя через порт Ethernet, который подключен через кроссовер UTP-кабеля, затем пересылает эти запросы на сервер VPN-ретрансляции предполагаемых получателей через интерфейс Wi-Fi. -Fi, интерфейс Wi-Fi, подключенный к точке доступа WLAN. В общем, AR-6000 служит для моста связи между пользователем ПК и внешней сетью, будь то для доступа в Интернет или удаленного доступа к внутренним ресурсам.

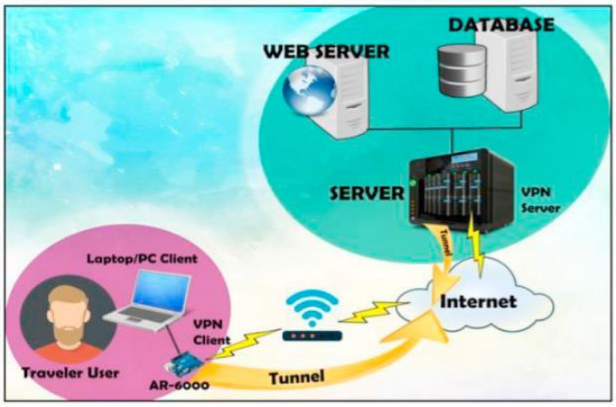


Figure 1 Portable VPN usage scenario (AR-6000)

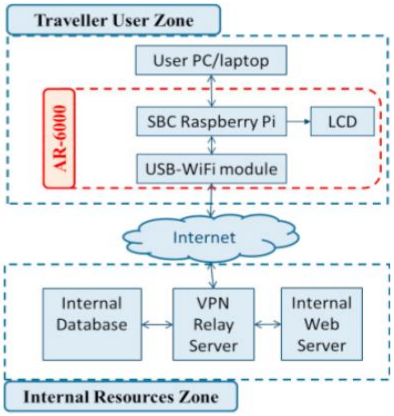


Figure 2 Hardware Design of AR-6000

Исходя из требований к дизайну, описанных в предыдущем подразделе, для реализации в пользовательской зоне путешественника и зоне внутренних ресурсов требуется немного оборудования, как показано на рис. 2. В пользовательской зоне путешественника используется пользовательский ПК / ноутбук и AR-6000. AR-6000 состоит из SBC Raspberry Pi 3 Model B + в качестве модуля микроконтроллера, модуля LCD для дисплея и модуля USB Wi-Fi в качестве средства связи. Микроконтроллер организует все функции прототипа AR-6000, например, управление связью с ПК пользователя, маршрутизация, переадресация IP, маскировка IP и т. д. OpenVPN-R устанавливается в качестве основных приложений в микроконтроллере. ЖК-модуль используется для отображения информации, такой как IP-порт Ethernet AR-6000, и для запуска приложения с помощью модуля с сенсорным экраном. Для подключения к Интернету AR-6000 оснащен модулем Wi-Fi в качестве средства связи с ближайшей точкой доступа WLAN. Пользовательский ПК выполняет запрос доступа к серверу ретрансляции VPN через AR-6000. Пользовательский ПК также может настроить AR-6000 через SSH-соединение. С другой стороны,

во внутренней зоне ресурсов есть 3 компонента, то есть сервер ретрансляции VPN, внутренняя база данных и внутренний веб-сервер. Сервер ретрансляции VPN - это компьютер, который используется в качестве цели удаленного доступа пользователя. Он получает и организует запрос удаленного доступа от AR-6000. Open VPN-R также устанавливается на сервере ретрансляции VPN, чтобы создать VPN-туннель к AR-6000 с шифротекстами Rabbit.

Разработка программного обеспечения

В этом разделе мы обсудим дизайн программного обеспечения для прототипа переносного VPN. Программный пакет является модификацией OpenVPN. Он называется Open VPN + R. Это программное обеспечение работает на SBC Raspberry Pi Model B + в качестве основных приложений VPN. Принципиальным отличием OpenVPN + R от оригинального OpenVPN является включение шифровальных наборов Rabbit в качестве альтернативного варианта шифровальных наборов TLS для защиты пути или канала данных транзакции. OpenVPN использует OpenSSL для криптографических алгоритмов и предоставления шифровальных пакетов TLS. Поэтому, чтобы добавить шифровальные наборы Rabbit в OpenVPN-R, необходимо реализовать алгоритмы для потоковых шифров Rabbit в OpenSSL и изменить OpenVPN, чтобы они могли распознавать алгоритм потокового шифра, который реализован в OpenSSL Rabbit.

Для осуществления реализации необходимо разработать новые наборы шифров TLS, которые представляют собой комбинацию нескольких криптографических алгоритмов с алгоритмом шифрования потока Кролика в качестве алгоритма шифрования данных (алгоритм массового шифрования). Комбинация криптографических алгоритмов состоит из алгоритмов аутентификации сервера, алгоритмов обмена ключами, алгоритмов шифрования данных и алгоритмов дайджеста сообщений. Новые наборы шифров TLS, сделанные в этом исследовании, относятся к стандарту протокола TLSv1.2 (RFC 5246), как определено в таблице 2.

Ciphersuites Rabbit	Authentication	Key Change	Encryption	Message Digest
TLS_RSA_WITH_RABBIT_SHA	RSA	RSA	RABBIT	SHA
TLS_DHE_DSS_WITH_RABBIT_SHA	DSS	DSS	RABBIT	SHA
TLS_DHE_RSA_WITH_RABBIT_SHA	RSA	RSA	RABBIT	SHA

Table 2 Protocol Ciphersuite Rabbit in Open VPN-R

В этом исследовании автор использует OpenSSL версии 1.0.2h, которая, как утверждается, успешно закрыла пробел в безопасности кровотечения. В общем случае реализация модификации исходного кода будет осуществляться как в библиотеках OpenSSL, так и в библиотеке криптографии и в библиотеке SSL. Добавления в библиотеку криптографии необходимы, потому что в этой библиотеке хранятся все криптографические функции, включая алгоритм шифрования потока Кролика, который будет реализован. Что касается библиотеки SSL, то основное внимание уделялось добавлению новых наборов шифров, в результате чего была реализована реализация SSL, поддерживающая использование алгоритма потокового шифра Rabbit. Его также необходимо изменить в некоторых скриптах компиляции, чтобы исходный код реализованного алгоритма потокового шифра Rabbit можно было интегрировать с OpenSSL. Результатом этого этапа реализации является версия OpenSSL 1.0.2h, которая загрузила алгоритм потокового шифра Rabbit в качестве одного из альтернативных вариантов алгоритма шифрования, как для кодирования на наборах TLS, так и для ручного кодирования через консольное приложение OpenSSL.

После завершения реализации алгоритма потокового шифра Rabbit, следующий будет изменен и перекомпилирован на OpenVPN для распознавания алгоритма потокового шифра Rabbit, реализованного в OpenSSL. OpenVPN, используемый в этом исследовании, является версией OpenVPN 2.3.10. Как только изменения в OpenVPN завершены, результатом является версия 2.3.10 OpenVPN, которая уже может распознавать алгоритм шифрования потока Кролика. Версия OpenVPN называется OpenVPN-R, которая будет использоваться в качестве основного приложения устройств AR-6000.

Список использованных источников:0

4.Choffnes D. A case for personal virtual networks. In: Proceedings of the 15th ACM Workshop on Hot Topics in Networks. 2016. p. 8– 14.

5.Alshalan A, Pisharody S, Huang D. A survey of mobile VPN technologies. IEEE Commun Surv Tutorials. 2016;18(2):1177–96.

6.Matotek D, Turnbull J, Lieverdink P. Networking with VPNs. In: Pro Linux System Administration. Springer; 2017. p. 701–31.

НОВЫЙ ПОДХОД К ПОВЫШЕНИЮ БЕЗОПАСНОСТИ MPLS VPN ПУТЕМ ПРИНЯТИЯ ПРОГРАММНО-ОПРЕДЕЛЯЕМОЙ СЕТЕВОЙ ПАРАДИГМЫ

Рубинштейн Р. Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Цветков В. Ю. – д. т. н., доцент

В работе рассмотрен новый подход к повышению безопасности MPLS VPN путем принятия программно-определяемой сетевой парадигмы

Безопасность сетевых инфраструктур является одной из утомительных задач в современных сетях. Действительно, в наши дни требуемая безопасность должна характеризовать динамизм и способность адаптироваться к контексту бирж, другими словами, безопасность не должна влиять на производительность сети. Чтобы удовлетворить эту потребность, можно использовать автоматизацию сети через контроллер программно-определяемой сети (SDN). SDN - новая парадигма, позволяющая через контроллер управлять всей архитектурой сети. В этой статье мы предлагаем новое решение для динамической генерации политик безопасности между различными сайтами MPLS VPN путем принятия подхода SDN. Безопасность является одной из основных задач бизнеса, поскольку безопасность - это не только конфиденциальность, целостность или аутентификация, но и высокая доступность. Высокая доступность зависит от нескольких факторов, а именно от используемого оборудования, стратегий и планов, предоставляемых компанией в случае неисправности системы. Иногда компании могут потребоваться четыре основных принципа безопасности, поэтому для поиска компромисса и решения, гарантирующего их, требуется много внимания. Например, протоколы шифрования или политики безопасности трафика в целом могут влиять на производительность оборудования и, таким образом, ставить под угрозу доступность ресурсов.

Многопротокольная коммутация по меткам «MPLS» рассматривается как основной протокол, развернутый на уровне ядра сети оператора. MPLS был успешным с появлением новых связанных сервисов, прежде всего сервиса виртуальной частной сети (VPN) . MPLS VPN позволяет получить безопасное соединение с меньшими затратами. Поэтому для создания клиентских VPN необходимо изолировать потоки каждого клиента.

Это правда, что MPLS VPN обеспечивает высокий уровень безопасности по сравнению с традиционными VPN, потому что трафик проходит через частную сеть оператора, но некоторые клиенты предпочитают добавлять уровень шифрования через протокол IPsec . IPsec также опирается на два протокола: 1) аббревиатуру заголовка аутентификации для AH, гарантирующую аутентификацию, целостность и защиту от повторного воспроизведения данных, 2) полезную нагрузку инкапсуляции "ESP", обеспечивающую большую конфиденциальность.

С появлением облака мы видим дополнительный шаг в автоматизации процессов с помощью Software Defined Network (SDN). Это значительно упрощает автоматизированные операции в стандартных и воспроизводимых средах. Благодаря этому новому режиму работы этапы тестирования и развертывания сокращены, что существенно экономит время и деньги. SDN позволяет по принципу оркестровки управлять сетевыми ресурсами компании из центральной точки, называемой контроллером. Парадигма SDN в нашей ситуации может быть принята для реализации новых правил для улучшения политик безопасности защищенных IPsec туннелей MPLS VPN с целью удовлетворения потребностей компании, особенно с точки зрения безопасности, целостности, аутентификации и особенно доступности.

Подход состоит из трех этапов: измерение производительности сети (приложения и оборудование), расчет соответствующей политики IPsec и развертывание этой политики на маршрутизаторах и устройствах. Эти шаги вращаются вокруг четырех элементов: доступность, конфиденциальность, целостность и аутентификация.

Список использованных источников:0

1. Bensalah, F., & El Kamoun, N. (2019). Novel software-defined network approach of flexible network adaptive for VPN MPLS traffic engineering. International Journal of Advanced Computer Science and Applications, 10(4), 280-284.

2. Bahnasse, A., Louhab, F. E., Ait Oulahyane, H., Talea, M., & Bakali, A. (2018). Novel SDN architecture for smart MPLS traffic engineering-DiffServ aware management. Future Generation Computer Systems, 87, 115-126.

СИСТЕМЫ МОНИТОРИНГА СЕТЕВОГО ОБОРУДОВАНИЯ СЕТИ WI-FI

Савичев А.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Цветков В.Ю. – доктор технических наук

В работе приведён сравнительный анализ существующих и свободно распространяемых систем мониторинга оборудования сети Wi-Fi. Сделаны выводы о явных преимуществах и недостатках сравниваемых систем.

1.Microsoft SCOM – System Center Operations Manager – система сквозного мониторинга от Microsoft, в том числе активного слежения за состоянием сетей (наблюдение за любыми сетевыми устройствами, поддерживающими SNMP, вплоть до уровня портов, а также обнаружение виртуальных локальных сетей и коммутаторов в таких сетях).

Основные достоинства:

– исключительная производительность и работоспособность приложений для программных сред Microsoft;

– обеспечивает сквозное управление службами для сервисов вашего центра обработки данных;

– способствует улучшению эффективности и управления средами центров обработки данных;

– унифицированный контроль в рамках частных и общедоступных облачных сервисов;

– поддержка Windows PowerShell 2.0 с набором новых командлетов;

Одно из главных достоинств System Center Operations Manager – продвинутая визуализация всего огромного собранного набора данных, в основном в виде графиков и диаграмм, причём визуализация доступна не только в специальной консоли программы, но и через веб-интерфейс.

Основные недостатки:

– система мониторинга охватывает множество общих показателей системы, но непригодна для слежения за специфическими параметрами;

– до сих пор работа с операционными системами вне семейства Windows нестабильна;

– необходимость установки сервиса агента;

– невероятная громоздкость и трудоёмкость настройки продукта «под себя»: система дольше подходит для мониторинга общего состояния и сбора основных сведений о большой структуре (например, множество клиентских и серверных машин в домене).

Также существенный недостаток системы состоит в высокой стоимости данного программного продукта.

2.Zabbix – свободно распространяемая система для комплексного мониторинга сетевого оборудования, серверов и сервисов.

Основные достоинства:

– вся конфигурация хранится в базе и управляется через веб-интерфейс;

– единая точка доступа для пользователей;

– разграничения доступа к данным и конфигурации;

– встроенные богатые средства визуализации;

– развитые возможности анализа собранных данных;

– предоставляет гибкие возможности по настройке условий-триггеров, которые включаются при авариях и неполадках;

Основные недостатки:

– все данные истории хранятся в базе, что неэффективно и ограничивает масштабируемость;

– не обеспечивается отказоустойчивость;

– мониторинг серверов и рабочих станций осуществляется через постоянно запущенный агент;

В качестве дополнительного минуса стоит отметить сложность делегирования прав – машина с сервисом зачастую управляется операционной системой семейства *nix, что делает трудоёмким взаимодействие с доменными пользователями и правами из Active Directory (Windows системы).

3.Nagios – (первоначально Netsaint) – свободно распространяемая программа для мониторинга систем и сетей.

Основные достоинства:

– простой формат конфигурационного файла. При наличии минимального опыта в программировании можно написать собственные плагины для Nagios;

– позволяет оставлять комментарии с меткой времени;

– существуют плагины на все случаи жизни от сторонних производителей;

– отправка оповещений в случае возникновения проблем со службой или хостом (с помощью почты, смс, или любым другим способом, определенным пользователем через модуль системы);

Основные недостатки:

– нет возможности конфигурирования через веб-интерфейс. Все изменения конфигурации выполняются правкой файлов конфигурации с последующим полным перезапуском сервера Nagios;

– слишком большой интервал между проверками и замерами параметров;

– отсутствуют встроенные средства визуализации (кроме карты сети);

– сложность масштабирования без использования плагинов от сторонних производителей;

– каждый плагин запускается как отдельный процесс;

Дополнительно к недостаткам можно отнести проблемное взаимодействие с серверами под управлением Windows.

4.Cacti – бесплатное приложение мониторинга, позволяющее собирать статические данные за определённые временные интервалы и отображать их в графическом виде при помощи RRDtool утилиты, предназначенной для работы с круговыми базами данных (Round Robin Database), которые используются для хранения информации об изменении одной или нескольких величин за определенный промежуток времени.

Основные достоинства:

– высокая скорость развертывания при минимальном дополнительном кодировании;

– простота и удобство интерфейса просмотра диаграмм и их настройки;

– возможность подключения скриптов;

Основные недостатки:

– сложен в первоначальной настройке;

– отсутствие возможности инвентаризации;

– ограниченная производительность «неродных» JMX решений для Cacti;

Так же отдельным недостатком можно выделить довольно быстрое нарастание количества однотипных настроек в случае большого числа сред и серверов.

5.Observium – является системой мониторинга и наблюдения за сетевыми устройствами и серверами. При этом список поддерживаемых устройств огромен и не ограничивается только сетевыми устройствами, главное условие — чтобы устройство поддерживало работу SNMP.

Основные достоинства:

– имеет огромнейший список систем, за которыми может производить мониторинг;

– предустановленные шаблоны для SNMP OID;

– отображение графиков, аппаратных ресурсов, датчиков в удобном для пользователя виде;

– подключение Syslog сообщений;

Основные недостатки:

– система оповещений доступна только в платной версии;

– работа с картами местности доступна только через Google карты;

– ограничен 5-ти минутным интервалом опроса устройств;

В результате анализа сравниваемых систем мониторинга выявлены следующие критические минусы:

– нет системы оповещений в Cacti;

– при использовании RRD в Cacti и Nagios теряется детализация старых данных;

– конфигурация в Nagios изменяется посредством изменения файла конфигурации, но новая конфигурация применяется только при перезапуске службы Nagios, что при большом количестве собираемых метрик может занимать несколько десятков минут, а следовательно, система не будет функционировать в это время.

Zabbix имеет менее критические недостатки, связанные с визуализацией данных, что слабо влияет на основные функциональные возможности системы. Наименее ресурсоемкой системой является Cacti и Observium, наиболее ресурсоемкой – Nagios и Zabbix. Но из-за описанных недостатков и необходимости использования большого количества сторонних плагинов для Cacti и Nagios, а также из-за сложности масштабирования этих систем наилучшим выбором для мониторинга большого количества метрик признан Zabbix и Observium.

Список использованных источников:

1. Основы мониторинга и сбора метрик. URL: https:// www.8host.com/blog/osnovy-monitoringa-i-sbora-metrik..
2. Шмелев В. В. Метод мониторинга технологических процессов на основе структурно-логического подхода // Интеллектуальные технологии на транспорте. 2017. № 2. С. 5-14.
3. Линикова О. Е. Мониторинг серверного оборудования и приложений. – Екатеринбург, 2014.

КОНТРОЛЬ МОДУЛЬНЫХ ОШИБОК ИТЕРАТИВНЫМИ КОДАМИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Симонович К.А.

Конопелько В.К. – д.т.н. профессор

Помехоустойчивое кодирование основано на введении, определенным образом, избыточной информации в передаваемые сообщения. Простым методом введения избыточности в передаваемые сообщения является метод "g" (g³3) - кратной передачи либо каждого информационного символа, либо всего блока в целом. Решение о каждом принятом информационном символе принимается по большинству одинаковых символов.
Таким образом, в результате 3-х кратной передачи блока из 5-ти двоичных символов была обнаружена и исправлена одиночная ошибка (3-й двоичный символ). Достоинством такого метода кодирования информации является его простота, а недостатком высокая избыточность информации; r = 66%.

Помехоустойчивое кодирование представляет собой процесс преобразования передаваемых информационных символов по определенному алгоритму или по определенным правилам, и в результате чего формируются последовательности кодовых символов, отображающие передаваемые информационные сообщения. В общем помехоустойчивое кодирование основывается на введении избыточной информации в передаваемые информационные сообщения. В результате помехоустойчивого кодирования формируются кодовые последовательности (кодовые слова, кодограммы) отображающие передаваемые информационные сообщения, которые условно делятся на разрешенные и запрещенные и по которым затем по определенным алгоритмам обнаруживаются и корректируются ошибочные информационные символы.

Основными характеристиками помехоустойчивых кодов являются:

1. Основание кода
2. Длина кодовой последовательности
3. Количество информационных символов
4. Скорость передачи кода
5. Избыточность помехоустойчивого кода
6. Вес кодовой последовательности
7. Классификация кодовых последовательностей
8. Кодовое расстояние

Источники:

1. **Норменное декодирование помехоустойчивых кодов и алгебраические уравнения**: монография / В.К.Конопелько, В.А.Липницкий. – Минск : Изд. Центр БГУ, 2007. – 239 с.

2. **Теория прикладного кодирования** : Учеб. Пособие. В 2 т. Т. 2/ В.К.Конопелько, В.А.Липницкий, В.Д.Дворников и др.; Под ред. Проф. В.К.Конопелько. – Мн.:БГУИР, 2004. – 398 с.

ОЦЕНКА ПОГРЕШНОСТИ ВОССТАНОВЛЕНИЯ НЕПРЕРЫВНЫХ СИГНАЛОВ ПО ДИСКРЕТНЫМ ДАННЫМ

Фам М.Т.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ильинков В.А. – канд.тех.наук, доцент

В настоящее время достаточно актуальным является вопрос наиболее точной передачи и восстановления сигналов. Для того, чтобы наиболее грамотно дать такую оценку как точность восстановления сигнала, необходимо определить следующую количественную меру как погрешность восстановления сигнала. В данной статье, для наиболее наглядной демонстрации будет рассмотрено восстановление непрерывных сигналов по соответствующим дискретным данным.

Пусть рассматриваемый непрерывный сигнал (процесс) будет представлен в виде последовательности его дискретных значений (1) в равноотстоящих точках $t_n = n\Delta t$:

$$u[n]=u(n\Delta t) \quad (1),$$

где n – порядковый номер отсчета, Δt – период времени.

Очевидно, что дискретный процесс лишь приблизительно отображает бесконечный непрерывный сигнал, и, в таком случае, требуется обозначить количественную меру данного приближения – найти погрешность дискретизации. Обычно под данной погрешностью процесса принимается та, с которой возможно восстановление непрерывного процесса по соответствующим ему дискретным значениям. Иными словами, под погрешностью дискретизации понимается погрешность в задаче интерполяции непрерывного процесса по заданным дискретным отсчетам. [1]

В целом, восстановление непрерывного сигнала (процесса) по соответствующему дискретному u[n] можно представить в виде пропускания последовательностей единичных импульсов (δ-функций) с огибающей u[n] и периодом времени Δt через линейный восстанавливающий элемент с некоторой импульсной переходной характеристикой $k_0(t)$, соответствующая процессу восстановления схема представлена на рисунке 1[2]

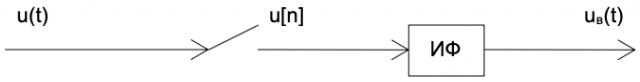


Рисунок 1 – Схема восстановления непрерывных процессов по дискретным данным с использованием восстанавливающего элемента (интерполирующего фильтра)

Стоит отметить, что, в общем случае, такого интерполирующего фильтра, который обеспечивает безошибочное восстановление стационарного случайного процесса, не существует.

В результате прохождения процесса восстановления образуется сигнал $u_в(t)$:

$$u_в(t)=\sum_{n=-\infty}^{\infty} u[n]k_0(t - n\Delta t) \quad (2).$$

Погрешность восстановления непрерывного сигнала посредством дискретизации, или ошибку интерполяции, в аналитическом виде выглядит следующим образом:

$$\Delta u(t)=u(t) - u_в(t) \quad (3).$$

также данную погрешность можно рассматривать в виде сигнала на выходе схемы, упомянутого на рисунке 1, при воздействии непрерывного сигнала, находящегося на входе схемы. [1]

Реальные же процессы, в отличие от непрерывных случайных, не имеют строго ограниченных спектров, поэтому и восстановление по дискретным отсчетам для них будут сопровождаться некоторыми ненулевыми погрешностями.

Список использованных источников:

1. Быков В.В Цифровое моделирование в статистической радиотехнике / В.В. Быков, М. : Советское радио, 1971, 328 с.
2. Левин Б.Р. Теоретические основы статистической радиотехники / Б.Р. Левин. – М. : Советское радио, 1969, т.1

ИСПОЛЬЗОВАНИЕ МОДУЛЯЦИИ ДЛЯ ПОВЫШЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ ПРИ ПЕРЕДАЧЕ СИГНАЛОВ ВОСП

Червяков А.И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Урядов В.Н. – к.т.н.,доцент

В настоящее время интенсивно развиваются исследования в области новых типов модуляции оптических сигналов, целью которых является увеличение эффективности волоконно-оптических сетей передачи (ВОСП), повышение помехоустойчивости, а также увеличение пропускной способности сети, что в конечном итоге приводит к снижению стоимости единицы передаваемой информации.

Долгое время в оптических сетях дальней связи удавалось увеличивать пропускную способность при сохранении дальности передачи информации. Сегодня в развитии DWDM-оборудования для городских и региональных сетей связи на первый план выходят две взаимосвязанные потребности:

• увеличение спектральной эффективности (рост скорости при той же занимаемой спектральной полосе), пусть даже и со снижением максимально достижимой дальности, – для повышения экономической эффективности использования доступного спектра;

• увеличение канальной скорости (в частности, предоставление клиенту интерфейсов 400 Гбит/с, 1 Тбит/с) – в связи с потенциальной стандартизацией и внедрением в будущем клиент ских каналов 400G Ethernet и 1T Ethernet.

Увеличение спектральной эффективности достигается главным образом за счет перехода к более сложным форматам модуляции – 8QAM, 16QAM, 64QAM. Неизбежной платой за это становится заметное снижение предельной дальности передачи без регенерации сигнала, что, впрочем, не является существенным недостатком для сетей городского и регионального масштабов.

Другой способ увеличения пропускной способности – повышение символьной скорости – ограничен физическими возможностями электроники и базовыми принципами связи.

В настоящее время активно развивается еще один способ увеличения канальной скорости – использование нескольких поднесущих (суперканалов). Он не приводит к росту эффективности использования спектра, но зато позволяет предоставить клиенту любую требуемую канальную скорость.

Три независимых пути увеличения канальной скорости систем связи – повышение символьной скорости, усложнение формата модуляции, использование нескольких поднесущих – показаны на рисунке 1. Канальная скорость рассчитывает ся как произведение значений по всем трем осям.

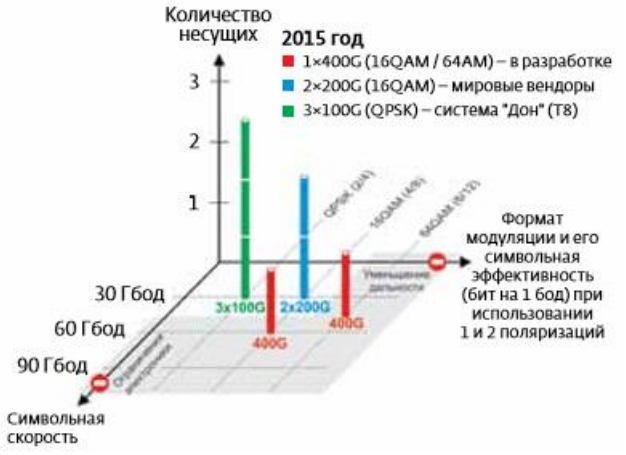


Рисунок 1 – Основные пути увеличения канальной скорости систем связи

Список использованных источников:

4. Конышев В.А., Леонов А.В., Наний О.Е., Трещиков В.Н., Убайдуллаев Р.Р. Рекордная производительность систем 100G как маркер перехода к эволюционному развитию ВОСП // Первая миля. 2015. № 6. С. 40– 43.

5. Леонов А.В., Слепцов М.Е., Трещиков В.Н. Развитие скоростных DWDM систем по нескольким поднесущим // Первая миля. 2016. № 2. С. 43– 47.

СПОСОБ ИДЕНТИФИКАЦИИ ДИСКРЕТНЫХ СИСТЕМ С ЗАПАЗДЫВАНИЕМ НА ОСНОВЕ ОБРАТНОГО *Z*-ПРЕОБРАЗОВАНИЯ

Шумский Д.Ю., Каретко А.С., Полубок А.Г., Левчук В.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Печень Т.М. – старший преподаватель

Рассматривается вопрос о необходимости параметрической компоновки при иденфикации систем с запаздыванием на основе обратного Z-преобразования. Анализируется оценка неизвестного времени задержки. Найдено модифицированное Z-преобразование для исследуемой дискретной системы.

Методика «Идентификации дискретных систем с запаздыванием на основе обратного Z-преобразования» заключается в решении следующих задач:

– Применить для параметрической идентификации в реальном масштабе времени (адаптивная или текущая идентификация, самонастройка) дискретных систем, описываемых регрессионной моделью:

$$y(k) = \sum_{i=1}^{n} a_i k_i (k-i) + \sum_{i=0}^{n} b_i x(k-i-d) + v(k),$$

где, $x(k), y(k)$ – входной и выходной сигналы; $v(k)$ – аддитивная помеха с нулевым средним и конечной дисперсией; n – порядок модели; d – запаздывание.

Для определения неизвестного запаздывания необходимо дополнительное уравнение, такое уравнение выводится на основе минимизации квадрата ошибки модели [1]*:*

$$e(k,d) = y(k|d) - y(k),$$

где $y(k|d)$ – выходной сигнал модели при значении запаздывания d.

– Решить следующую задачу: так как в задаче текущей идентификации определяется вектор параметров передаточной функции дискретной системы, то формально задача оценки неизвестного запаздывания τ сводится к обратному *Z*-преобразованию.

В дискретной системе запаздывание нижняя частота представляется в виде целого числа интервалов квантования (T_0).

Определяем запаздывание как:

$$\tau = (d + m - 1)T_0 = (d - \varepsilon)$$

где $m[0,1)$, $\varepsilon(0,1]$ — дробные числа, *d* — целое, m и ε связаны соотношением $m = 1 - \varepsilon$.

– Найти модифицированное *Z*-преобразование рассматриваемой дискретной системы:

$$H(z) = \frac{z}{z-1}\frac{B(z)}{A(z)} = Z_s\left\{\frac{1}{s}\frac{B^*(s)}{A^*(s)}\right\} = Z_s\{H^*(s)\},$$

и обратное модифицированное *Z*-преобразование:

$$H^*(s) = Z_s^{-1}\{H(z)\},$$

При текущей параметрической идентификации на каждом шаге самонастройки оценивается вектор параметров $\theta(k)$ передаточной функции дискретной системы при уже известном запаздывании *d*. Параметр смещения ε не известен, а следовательно, и запаздывание τ не определено с точностью дробной части.

– Составить дополнительное уравнение для параметра ε:

$$F(\varepsilon) = \sum_{i=1}^{l} \sum_{j=0}^{r_i-1} G_{ji}^{*} (-\varepsilon)^j z_i^{-s} = 0$$

Данное уравнение связывает известные параметры передаточной функции дискретной системы с неизвестным значением ε.

– Получить явную зависимость в частном случае для инерционного звена первого порядка с запаздывание:

$$\varepsilon = \ln\left(\frac{b_0 + b_1}{b_1 - a_1 b_0}\right) \Big/ \ln(-a_1)$$

– Решить соотношения :

$$\left.\begin{aligned} G_{ji}^{*} &= (-1)^{j+1} \sum_{q=j}^{r_i-1} G_{qi} \frac{S(q+1, j+1)}{q!} z_i^{q+1}; \\ G_{ji}^{*} &= z_i^{s} \sum_{g=j}^{r_i-1} D_{qi} \frac{C_q^j}{q!} T_0^q \varepsilon^{q-j}; \\ i &= \overline{1, l}; j = \overline{j = 0, r_i - 1}, \end{aligned}\right\}$$

Эти соотношения позволяют сформировать систему линейных уравнений для вектора коэффициентов $\boldsymbol{D} = \|D_{ji}\|$при обратном модифицированном *Z*-преобразовании и вектора коэффициентов $\boldsymbol{G} = \|G_{ji}\|$при прямом модифицированном *Z*-преобразовании $\boldsymbol{G} \leftrightarrow \boldsymbol{G}^{*} \leftrightarrow \boldsymbol{D}$ алгоритмы разложения рациональной дроби на сумму простых дробей позволяют применять матричные операции к вектору параметров $\theta(k)$.

– При прямом и обратном модифицируемом Z-преобразовании формализовать оператор [2]:

$$\theta = Z(\varepsilon, \boldsymbol{D}),\ D = Z^{-1}(\varepsilon, \theta).$$

– Сформировать матрицы ковариаций при изменении запаздывания. При этом запаздывание и порядок передаточной функции дискретной системы относятся к структуре цифровой модели. Если структура изменяется, то параметрическая идентификация должна начинаться с формирования новой системы уравнений.

– Представить вычислительную схему рекуррентного метода наименьших квадратов в виде прямого обращения ковариационной матрицы и записать:

$$R(k, d)\theta(k, d) = F(k, d)$$

– Пересчитать матрицу ковариаций $R(k, d)$ в матрицу $R(k, d+1)$. Матрицы $R(k, d)$ и $R(k, d+1)$ содержат одинаковые блоки. Одинаковые блоки выделить и в матрицах $R(k-1, d)$ и $R(k, d+1)$. С учетом перекрытия блоков и симметричности матрицы ковариаций «не закрытыми» остается лишь один элемент матрицы $R(k, d+1) - r_{2n+1,1}(k, d+1)$(рис. 1).

$$R(k, d+1) = \begin{bmatrix} A_1(k) & A_2(k, d) & r_{1,2n+1}(k, d+1) \\ & & B_{2n+1}(k-1, d) \\ A_2^T(k, d) & & \\ r_{2n+1,1}(k, d+1) & B_{2,n+1}^T(k-1, d) & B_3(k-1, d) \end{bmatrix}$$

Рисунок 1 – Матрица ковариаций

Таким образом, предложен разработанный на основе рекуррентного метода наименьших квадратов алгоритм текущей идентификации объектов управления с переменным запаздыванием, описываемых дискретной системой, состоящей из идеального импульсного элемента, экстраполятора нулевого порядка и линейной непрерывной части. Алгоритм не накладывает

дополнительных ограничений на синтез систем управления и может применяться в замкнутом контуре.

Список использованных источников:

1. Льюнг Л. Идентификация систем. Теория для пользователя / Пер. с англ.; под ред. Я. З. Цыпкина. М.: Наука, 1991. 432с.

2. Карташов В.Я., Сахнин Д. Ю. Структурно-параметрическая идентификация дискретных моделей объектов с запаздыванием для настройки регуляторов Смита // Управление, вычислительная техника и информатика: Изв. Томск. политехн. ун-та. 2007. Т. 311, № 5. С. 19—23.