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

ИНФОКОММУНИКАЦИИ

**55-я юбилейная научная конференция
аспирантов, магистрантов и студентов**

Сборник тезисов докладов

22–26 апреля 2019 года
Минск, БГУИР

УДК 621.391

Инфокоммуникации: 55-я юбилейная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 22-26 апреля 2019 г., БГУИР, Минск, Беларусь: тезисы докладов. – Мн. – 2019. – 104 с.; ил.

В сборнике опубликованы тезисы докладов, представленных на 55-й юбилейной 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

ЭЛЕКТРОННАЯ СТАБИЛИЗАЦИЯ ВИДЕОИЗОБРАЖЕНИЯ С НЕСТАЦИОНАРНОЙ КАМЕРЫ

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

Пчёлкин А.С.

Черная И.И. – к.т.н., доцент каф. ЗИ

Техники видеостабилизации имеют принципиальное значение для большинства видеопоследовательностей снятых с нестационарных камер из-за высокочастотных помех. Некоторые алгоритмы стабилизации, основанные на 2D и 3D преобразованиях, хорошо изучены, однако было предложено мало решений на базе глубоких нейронных сетей. В данной статье предложен алгоритм видеостабилизации с использованием сверточных нейронных сетей.

Предложенная модель *StabNet* является сверточной нейронной сетью (СНС), которая обучается прогнозировать параметры трансформации для каждого входящего необработанного кадра на основе набора обработанных кадров. Применение полученных параметров трансформации к входному необработанному кадру генерирует стабилизированный выходной кадр. Стабилизированных кадр помещается в набор обработанных кадров для стабилизации последующих необработанных кадров. На рисунке 1 показана схема предложенной модели *StabNet.*

Рис.1 – Схема модели *StabNet*

Архитектура сети показана рисунке 2. *StabNet* это сиамская сеть с двумя ветвями с обзими параметрами для обеих ветвей. Сеть состоит из кодировщика и гомографического регрессора. Гомографический регрессор это 8-канальный выходной сверточный слой с размером ядра 1×1 и шагом 1 пиксел(k1n8s1). Во время обучения, 2 последовательных кадра подаются на вход сети и прогнозируются параметры трансформации. При обучении используются функция потери устойчивости и функция временных потерь.

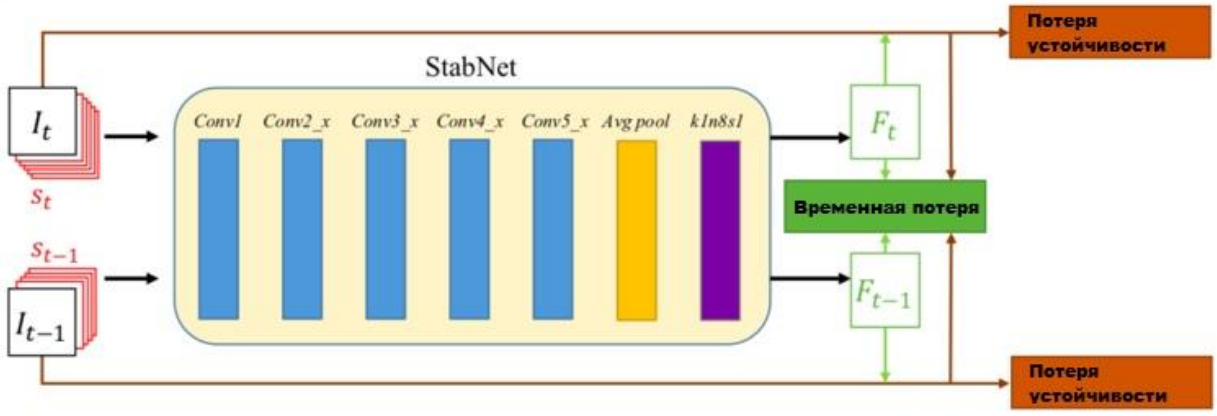


Рис. 2 – Архитектура сети

Функция потерь:

$$L = \sum_{i \in \{t, t-1\}} L_{stab}(F_i, I_i) + \delta L_{temp}(F_t, F_{t-1}, I_t, I_{t-1})$$

Функция потерь устойчивости:

$$L_{stab}(F_t, I_t) = L_{pixel}(F_t, I_t) + \alpha L_{feature}(F_t, I_t),$$

$$L_{pixel}(F_t, I_t) = \frac{1}{D}\|I'_t - F_t * I_t\|_2^2.$$

где I'_t – прямые наблюдения,

D – размерность кадра.

$$L_{feature}(F_t, I_t) = \frac{1}{m}\sum_{i=1}^{m}\left\|p'^i_t - F_t * p^i_t\right\|_2^2,$$

$$P_t = \left\{\langle p^i_t, p'^i_t\rangle \middle| i \in \{1, \dots, m\}\right\},$$

где m – пары совпавших особых точек между необработанным/обработанным кадром.

Функция временных потерь:

$$L_{temp}(F_t, F_{t-1}, I_t, I_{t-1}) = \frac{1}{D}\|F_t * I_t - \omega(F_{t-1} * I_{t-1})\|_2^2,$$

где $\omega(\cdot)$ - функция, преобразующая обработанный кадр t-1 к обработанному кадру t согласно заранее вычисленному оптическому потоку.

Результаты экспериментов показывают, что предложенная модель демонстрирует сравнимые результаты с более изученными методами, при этом работая в 30 раз быстрее. Также StabNet справляется с ночными и размытыми видеопоследовательностями, с которыми у традиционных методов часто возникают трудности.

Список использованных источников:

1.Ганина Я.В.Семантическая сегментация изображений на основе метода машинного обучения// Дипломная работа. - Москва, 2011-63с.

2. Фурман. Я.А. Введение в контурный анализ; приложения к обработке изображений и сигналов/ Я. А. Фурман, А. К. Кревецкий, А.К. Передреев// Научное издание. – Москва, 2003-592с

МЕТОДЫ МОНИТОРИНГА КЛАСТЕРНЫХ СЕРВИСОВ В ОБЛАСТИ ЭЛЕКТРОННОЙ КОМЕРЦИИ

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

Жук П.Б., Бобов М.Н.

В этой работе рассмотрены основные метрики и методы, применяемые для мониторинга кластерных сервисов в области электронной коммерции.

В настоящее время для обеспечения высокой доступности веб-сервисов, масштабирования, балансирования трафика, данных между несколькими серверами широко используется подход размещения одного сервиса в кластере серверов.

При таком подходе понимание состояния инфраструктуры и систем важно для стабильной работы сервисов. Информация о работоспособности и производительности развертываний не только помогает вовремя реагировать на проблемы, но и дает возможность уверенно вносить все требуемые изменения. Один из способов получить эту информацию – это система мониторинга, позволяющая осуществлять сбор метрик, визуализацию данных и нотификацию в случае неправильной работы кластерных сервисов.

Мониторинг – это процесс сбора, агрегирования и анализа этих данных для улучшения понимания характеристик и поведения компонентов системы. Данные из разных точек среды собираются системой мониторинга, которая отвечает за хранение, агрегацию, визуализацию данных и автоматические реагирует на изменения, когда значения соответствует заданным условиям.

Метрики, мониторинг и система оповещений составляют основу системы мониторинга и позволяют отразить состояние системы, отследить тенденции в потреблении ресурсов или поведении, а также влияние вносимых изменений.

Одной из функций систем мониторинга является организация и корреляция данных из различных источников. Эффективность показателей мониторинга можно оценить возможностью администратора шаблоны поведения между разными ресурсами и группами серверов.

В основном, выделяют четыре вида метрики для осуществления мониторинга: задержка ответа сервиса, уровень входящего трафика, ошибки, занятость ресурсов.

Задержка – это время, необходимое для завершения действия. Специфика измерения этой метрики зависит от компонента, ее общие аналоги – время обработки, время отклика.

Задержка показывает, как долго будет выполняться конкретная задача или действие. Измерение задержки различных компонентов позволяет построить целостную модель различных характеристик системы. Это может помочь найти узкие места и определить каким ресурсам нужно больше всего времени, и своевременно обратить внимание на замедление работы системы. Следует подчеркнуть, что при расчете задержек важно учитывать как успешные, так и неуспешные запросы, поскольку они могут искажать средние значения сервиса.

Уровень трафика обозначает занятость ресурсов системы. Это нагрузка на сервисы, которая позволяет определить количество входящего и исходящего трафика, обрабатываемого системой в настоящее время.

Ошибки и их количество позволяют иметь более полную картину состояния компонентов и их реакции на запросы. Разделяя различные типы ошибок, возможно более точно определить проблемы, влияющие на приложения. Это также позволяет настроить гибкую систему оповещений: об отдельных типах ошибок система может оповещать немедленно, а другие игнорировать, пока они не превышают определенный порог.

Данные **использования ресурсов** предоставляют информацию о ресурсах, от которых зависит эффективность сервиса. Поскольку работа сервиса, который предоставлен одним компонентом, может требоваться для работы другого сервиса, использование ресурсов является одним из важнейших показателей для определения проблем с пропускной способностью. Проблемы использования ресурсов и задержки в одном слое могут отображать существенный скачок трафика или наличие ошибок в нижнем слое.

На основании вышеперечисленных метрик существует 2 метода мониторинга кластерных сервисов: USE и RED.

USE (utilization, saturation, errors) метод предназначен для выявления проблем в производительности ресурсов и основан на измерении трех основных метрик использование ресурсов:

1) Использование (англ. utilization) – время, в течение которого ресурс был занят обработкой полезного трафика.
2) Насыщение (англ. saturation) – степень загруженности ресурса, т.е. отношение необработанного трафика к обработанному.

3) Ошибки (англ. errors) – количество ошибок при обработке.

RED (rate, errors, duration) метод сосредоточен на выявлении ошибок, не связанных в большинстве с производительности (ошибки логики программы, неправильной конфигурации) и основан на трех метриках.

1) Темп (англ. rate) – количество успешно обработанных запросов за единицу времени.
2) Ошибки (англ. errors) – количество неудачно обработанных запросов за единицу времени.
3) Длительность (англ. duration) – интервал времени, необходимый для обработки запроса.

Оба метода обеспечивают оценку работы кластерных сервисов, однако только совместное использование данных методов может обеспечить более высокий уровень качества мониторинга сервисов.

Список использованных источников:
1. Newman, S. Building Microservices // O'Reilly Media, Inc. – 2016 – Piter Press Ltd.– P. 197 - 205
2. Beyer, B. Site Reliability Engineering. / C. Jones, J. Petoff, N. R. Murphy // O'Reilly Media, Inc. – 2016 – P. 50 – 67

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ДИНАМИЧЕСКОЙ И СТАТИЧЕСКОЙ МАРШРУТИЗАЦИИ

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

Романенко О.А.

Мухуров Н.И. – д.т.н.,профессор

Маршрутизация является одной из наиболее важных процедур передачи данных. Это гарантирует то, что данные перемещаются из одной сети в другую с оптимальной скоростью и минимальной задержкой, и что при этом сохраняется целостность в этом процессе. В работе проведен краткий обзор и сравнительный анализ статической и динамической маршрутизации, а также сделаны выводы о целесообразности использования каждого из них.

Статическая маршрутизация – вид маршрутизации, при котором маршруты указываются администратором в явном виде при настройке маршрутизатора [1]. Маршрутизация при этом осуществляется без участия каких-либо протоколов маршрутизации. Статические маршруты весьма распространены, поскольку они не требуют такого количества операций и вычислений, как протоколы динамической маршрутизации. Стоит отметить, что статическая маршрутизация уменьшает количество передаваемой служебной информации, поскольку в этом случае не посылается информация об изменениях в маршрутном расписании [2].

Статическая маршрутизация имеет три основных назначения:

1) обеспечение упрощённого обслуживания таблиц маршрутизации в небольших сетях, где не планируется расширение[3];

2) маршрутизация к тупиковым сетям и от них (тупиковая сеть представляет собой сеть, доступ к которой осуществляется через один маршрут, и маршрутизатор имеет только одно соседнее устройство);

3) использование маршрута по умолчанию для предоставления пути к любой сети, не имеющего более точного совпадения с другим маршрутом в таблице маршрутизации. Маршруты по умолчанию используются для отправки трафика в любой пункт назначения за пределами следующего маршрутизатора.

Преимуществами статической маршрутизации являются:

– статические маршруты не объявляются по сети, таким образом, они более безопасны;

– статические маршруты используют более узкую полосу пропускания, чем протоколы динамической маршрутизации. Кроме того, для расчёта и связи маршрутов не требуются ресурсы центрального процессора;

– путь, используемый статическим маршрутом для отправки данных, известен.

Недостатками статической маршрутизации являются:

– исходная настройка и дальнейшее обслуживание требуют временных затрат;

– при настройке часто допускаются ошибки (в наибольшей степени этот недостаток заметен при настройке статической маршрутизации в больших сетях);

– для изменения маршрута требуется вмешательство сетевого администратора;

– недостаточные возможности масштабирования для растущих сетей, поскольку обслуживание становится довольно трудоёмким;

– для качественного внедрения требуется доскональное знание всей сети.

Статические маршруты рекомендуется использовать в небольших сетях, для которых задан только один путь к внешней сети. Они также обеспечивают безопасность в больших сетях с определённым типом трафика или в каналах к другим сетям, для которых требуются расширенные функции контроля.

Динамическая маршрутизация – вид маршрутизации, при котором таблица маршрутизации редактируется программно. В UNIX-системах демонами маршрутизации; в других системах – служебными программами.

При динамической маршрутизации происходит обмен маршрутной информацией между соседними маршрутизаторами, в ходе которого они сообщают друг другу, какие сети в данный момент доступны через них. Информация обрабатывается и помещается в таблицу маршрутизации [4]. Протоколы маршрутизации позволяют маршрутизаторам динамически обмениваться данными об удалённых сетях и автоматически добавлять эти данные в таблицы маршрутизации.

Протоколы динамической маршрутизации используются для решения ряда задач:

1) обнаружение удаленных сетей;

2) обновление данных маршрутизации;

3) выбор оптимального пути к сетям назначения;

4) поиск нового оптимального пути в случае недоступности текущего пути.

Протоколы маршрутизации определяют оптимальный путь или маршрут к каждой сети. Затем маршрут добавляется в таблицу маршрутизации. Основным преимуществом протоколов динамической маршрутизации является то, что они обеспечивают обмен данными маршрутизации

между маршрутизаторами в случаях изменений топологии сети. Подобный обмен данными позволяет маршрутизаторам автоматически получать информацию о новых сетях, а также находить альтернативные пути в случае отказа канала в текущей сети.

Преимуществами динамической маршрутизации являются:

– подходит для работы во всех топологиях, где требуется наличие нескольких маршрутов;

– как правило, не зависит от размеров сети;

– автоматически изменяет таблицу маршрутизации при изменении сетевой топологии.

Недостатками динамической маршрутизации являются:

– реализация может предполагать высокий уровень сложности;

– требуется знание дополнительных команд для реализации;

– менее безопасна (для обеспечения высокого уровня безопасности требуется дополнительная настройка);

– маршрут зависит от текущей топологии;

– требуются дополнительные ресурсы центрального процессора, оперативного запоминающего устройства и полосы пропускания канала.

Протоколы динамической маршрутизации идеально подходят для сетей любого типа, содержащих несколько маршрутизаторов, поскольку обеспечивают высокий уровень масштабируемости, а также автоматически определяют оптимальные маршруты при изменениях в топологии. Несмотря на то, что настройка протоколов динамической маршрутизации требует больше временных затрат, их проще настраивать в рамках большой сети. По сравнению со статической маршрутизацией протоколы динамической маршрутизации требуют меньшего вмешательства со стороны сетевого администратора. Тем не менее, к издержкам использования протоколов динамической маршрутизации можно отнести тот факт, что часть ресурсов маршрутизатора выделяется для работы протокола.

Сравнительная характеристика динамической и статической маршрутизации приведена в таблице 1.

Таблица 1 – Сравнительная характеристика динамической и статической маршрутизации

Параметр	Статическая маршрутизация	Динамическая маршрутизация
Сложность настройки	Повышается с увеличением размера сети	Как правило, не зависит от размера сети
Изменение топологии сети	Требуется вмешательство сетевого администратора	Изменяется автоматически при изменении топологии сети
Масштабирование	Подходит для простых топологий	Подходит для простых и сложных топологий
Безопасность	Более высокий уровень безопасности	Более низкий уровень безопасности
Потребление ресурсов	Не требует дополнительных ресурсов	Использует центральный процессор, память и полосу пропускания канала
Предсказуемость маршрута	Маршрут к месту назначения всегда один и тот же	Маршрут зависит от текущей топологии

Несмотря на преимущества динамической маршрутизации, статическая маршрутизация по-прежнему находит широкое применение. В некоторых случаях рекомендуется использовать именно статическую маршрутизацию, равно как в других случаях предпочтительней применять динамическую маршрутизацию. Для сетей среднего уровня подходит как статическая, так и динамическая маршрутизация. Важно отметить, что статическая и динамическая маршрутизация не являются взаимоисключающими. В большинстве сетей используется комбинация статических маршрутов и протоколов динамической маршрутизации.

Список использованных источников:

1. xgu.ru [Электронный ресурс]. – Режим доступа: http://xgu.ru/wiki/Статическая_маршрутизация – Дата доступа: 23.03.2019.

2. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство. Пер.с англ. – М.: ООО "И.Д. Вильямс", 2007. – 994с

3. cloud.mppl.mk.ua [Электронный ресурс]. – Режим доступа: http://cloud.mppl.mk.ua/ccna.mppl.mk.ua/CCNA 2 RUS – Дата доступа: 23.03.2019.

4. helpiks.org [Электронный ресурс]. – Режим доступа: https://helpiks.org/9-20149.html – Дата доступа: 23.03.2019.

СИСТЕМА МОНИТОРИНГА БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ НА ОСНОВЕ АНАЛИЗА СОБЫТИЙ

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

Сороко М.В.

Астровский И.И. – к.т.н., доцент

Любая корпоративная компьютерная сеть, даже небольшая, требует постоянного внимания к себе. Как бы хорошо она ни была настроена, насколько бы надежное ПО не было установлено на серверах и клиентских компьютерах – нельзя полагаться лишь на внимание системного администратора; необходимы автоматические и непрерывно действующие средства контроля состояния сети и своевременного оповещения о возможных проблемах. Также особое внимание необходимо уделять постоянному мониторингу событий, связанных с безопасностью информационных систем.

Системы защиты постоянно развиваются и адаптируются к новым видам угроз. Количество источников информации, из которых поступают данные по текущему состоянию защищенности, растет с каждым днем. Когда инфраструктура слишком сложна, невозможно уследить за общей картиной происходящего в ней. Если своевременно не реагировать на возникающие угрозы и не предотвращать их, толку не будет даже от сотни систем безопасности. На помощь приходят системы управления событиями информационной безопасности – Security Information and Event Management (SIEM) [1].

SIEM - это технология, которая помогает в мониторинге, предупреждает администратора, коррелирует события журналов безопасности, позволяет расследовать инциденты, позволяет строить отчетность. SIEM может служить, как хранилище журналов для дальнейшего анализа.

Система управления событиями может помочь компании в повседневном оперативном мониторинге сетевых устройств, компьютеров, серверов, веб-сайтов, службы каталогов (Active Directory) и других устройств, которые используются в корпоративных сетях. Таким образом с помощью системы управления событиями можно построить единый центр реагирования в компании – Security Operation Center(SOC), который станет основным инструментом для анализа и поддержания состояния безопасности на достаточно высоком уровне [2].

Для внедрения данных систем необходимо провести ряд первоначальных мероприятий:

-Оценить инфраструктуру предприятия

-Определить количество источников, с которых будут собираться журналы безопасности

-Определить способы и протоколы передачи журналов на сервер

-Рассчитать среднее количество событий в минуту со всех источников

Главным этапом в построении систем мониторинга является правильный выбор источников событий. Рассмотрим основные источники:

-Сервера управления доступом — для мониторинга контроля доступа к информационным системам и использования привилегий

-Журналы событий серверов и рабочих станций

-Сетевое оборудование, маршрутизаторы, межсетевые экраны

-Системы предотвращения вторжений

-Сервера антивирусной защиты. События о работоспособности ПО, баз данных, изменении конфигураций и политик, вредоносных программах

-Сканеры уязвимостей

-Системы предотвращения утечек информации, антифрода

-Netflow и системы учета трафика

Заключительным этапом внедрения SIEM систем является настройка правил безопасности, так как корректно настроенные правила позволяют администраторам реагировать на инциденты в минимально кратчайшие сроки.

Список использованных источников:
1. SIEM [Электронный ресурс] – Режим доступа: https://www.securitylab.ru/analytics/430777.php
2. CISSP All-In-One Exam Guide // Шон Харрис – 2011

АЛГОРИТМ СЖАТИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ КОДИРОВАНИЯ ДЛИН СЕРИЙ ДЛЯ ПОЛУТОНОВЫХ ИЗОБРАЖЕНИЙ

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

Данильчик М. М.

Цветков В. Ю.. – д.т.н.,профессор

В настоящее время задача исследования и разработки методов сжатия информации является актуальной задачей, научной и прикладной. Наиболее актуальной она является в условиях ограниченных вычислительных и временных ресурсов. В таких условиях становится целесообразно использовать алгоритмы сжатия на основе кодирования длин серий.

Кодирование длин серий (run-length encoding, RLE) – или кодирование повторов — алгоритм сжатия данных, заменяющий повторяющиеся символы (серии) на один символ и число его повторов. Серией называется последовательность, состоящая из нескольких одинаковых символов [1]. Само сжатие в RLE происходит за счет того, что в исходном изображении встречаются цепочки одинаковых байт [2].

Как правило, изображения состоят из пикселов, соседние значения которых мало отличаются. Этот факт является предпосылкой к созданию алгоритма на основе кодирования длин серий, который учитывает малое изменение соседних элементов изображения.

Блок-схема модифицированного алгоритма RLE представлена на рисунке 1.

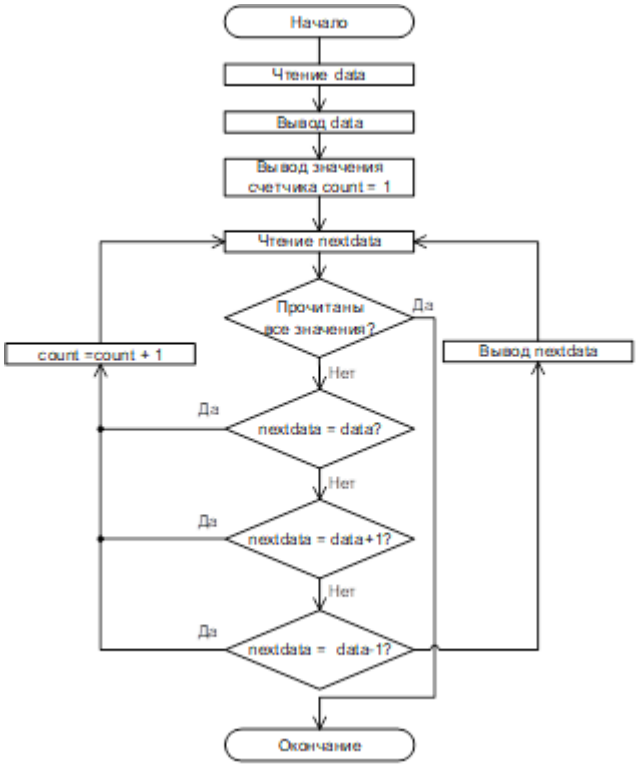


Рисунок 1 – Блок-схема алгоритма RLE с потерями

На первом этапе происходит чтение пикселя изображения data и инициализация счетчика. Далее считывается следующий пиксель и сравнивается с предыдущим, и, если он отличается не больше, чем на единицу, то значение счетчика возрастает на единицу. Данный алгоритм позволяет сжимать длинные серии пикселей изображения с практически не меняющимися значениями.

Разработанный алгоритм обеспечивает лучшую степень сжатия по сравнению с классическим алгоритмом RLE и мало уступает по времени выполнения. Данный алгоритм хорошо реализуется на программируемых логических интегральных схемах (ПЛИС), позволяя получить сравнимое с RLE быстродействие. Основной недостаток – данный алгоритм является алгоритмом сжатия с потерями, также, как и классический RLE, плохо сжимает изображения с резкими переходами.

В дальнейшей работе планируется модификация данного алгоритма.

Список использованных источников:

1. Сэломон, М. Сжатие данных, изображений и звука / М. Сэломон. – М. : Техносфера, 2004. – 368 с.
2. Ватолин Д. С. Алгоритмы сжатия изображений / Д. С. Ватолин. – М. : МГУ, 1999. – 76 с.

KALI LINUX В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Михейчик А.Д.

Хацкевич О.А. – к. т. н., доцент

В работе рассмотрен один из самых известных инструментов, служащий для проведения тестирования на проникновение, - дистрибутив Kali Linux. Продемонстрированы его недостатки, а также известные инструменты, с помощью которых специалисты по защите информации могут проводить испытания.

На сегодняшний день использование новейших сервисов и технологий приводит к эффективному функционированию информационной среды. Но, к сожалению, данные сервисы и технологии могут быть уязвимы для кибератак, что может привести к серьезным последствиям. К таким последствиям можно отнести: осуществление DDoS-атак; кража конфиденциальной информации; проникновение вредоносных программ, которые могут непосредственно повлиять на работу компании и т.д.

Для решения проблем, связанных с информационной безопасностью, многие компании устанавливают антивирусные программные средства, межсетевые экраны, системы обнаружения и предотвращения вторжений, DLP-системы и т.п. В последнее время набирает популярность тестирование на проникновение (пентестинг).

Пентестинг представляет из себя инструмент, с помощью которого осуществляется серия тестов на проникновение, которые основаны на атаках информационной системы для того, чтобы обнаружить недостатки и слабые места данной системы и в последствии их устранить [1]. Следует учитывать, что данные тесты не наносят вред информационной системе.

На данный момент существует большое разнообразие инструментов, с помощью которых можно выполнить тестирование на проникновение. Благодаря тому, что многие инструменты используются отдельно, возник вопрос о том, чтобы их объединить в одну систему. К такой системе можно отнести и известный дистрибутив Linux – Kali Linux.

Данный дистрибутив служит для специалистов по защите информации, чтобы тестировать систему на безопасность. В виду того, что для работы с инструментами, которые встроены в Kali, нужно иметь права суперпользователя, то уровень пользователя по умолчанию является root. Следовательно, это одна из веских причин, почему не стоит использовать данный дистрибутив для обычного пользования.

Как уже отмечалось выше, Kali Linux используется только для осуществления пентестинга, поэтому все программы, которые встроены в данный дистрибутив, служат только для тестирования безопасности. В нем отсутствуют обычные офисные программы, читалки и т.п. Инструменты, которые могут быть использованы, представлены на рисунке 1 [2].

Рисунок 1 – Инструменты Kali Linux

Ниже будет дана краткая характеристика пяти известных инструментов, которые установлены по умолчанию в дистрибутиве Kali [3]:

1) Jhon The Ripper – инструмент, который используется специалистами для взлома паролей методом перебора;

2) Aircrack-ng – эта программа предназначена для взлома и тестирования безопасности Wi-Fi сетей;

3) Burp Suite – инструмент служит для обнаружения уязвимостей на сайтах Интернета и веб-приложений, которые работают по HTTP и HTTPS протоколам;

4) Wireshark – один из самых известных инструментов, служащий для проведения анализа сетевых пакетов, приложений;

5) Metasploit – платформа для разработки, тестирования и использования кодов эксплойтов.

В статье рассмотрены проблемы информационной безопасности. Предложено использовать известный дистрибутив Kali Linux для проведения тестирования информационной системы на проникновение. Продемонстрированы известные инструменты, которые входят в состав Kali, используемые специалистами для проведения испытаний.

Список использованных источников:

1. Пентестинг [Электронный ресурс] – Режим доступа: http://www.tadviser.ru (Дата обращения: 17.03.2019).

2. Kali Linux [Электронный ресурс] – Режим доступа: https://losst.ru/obzor-kali-linux (Дата обращения: 18.03.2019).

3. Инструменты Kali Linux [Электронный ресурс] – Режим доступа: https://losst.ru/luchshie-instrumenty-kali-linux (Дата обращения: 19.03.2019).

СМЯГЧЕНИЕ ПИЛОТНОГО ЗАГРЯЗНЕНИЯ ЧЕРЕЗ КОНФИГУРАЦИЮ АНТЕННЫ БАЗОВОЙ СТАНЦИИ В WCDMA

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

Сакович Д.А.
Аксёнов В.А. – старший преподаватель

В этой работе цель состоит в том, чтобы оценить, сколько пилотно загрязненных территорий можно уменьшить с помощью традиционного метода планирования радиосети как выбор диаграммы направленности и наклона антенны.

Пилотное загрязнение наблюдается в районах, где мобильным станциям не хватает RAKE для обработки всех принятых пилот-сигналов или в них отсутствует доминирующий пилот-сигнал. Эта работа оценивает влияние конфигурации антенны базовой станции в 3-х секционных и в 6-ти разных WCDMA сайтах на количество пилотно загрязненных территорий. В WCDMA (широкополосный множественный доступ с кодовым разделением) система как UMTS (универсальная мобильная система связи), мобильные телефоны в сети могут идентифицировать различные сектора базовой станции в соответствии с их основным общим канальным пилот-сигналом (P-CPICH) [1]. Сигнал CPICH является предопределенной последовательностью символов, и она используется в качестве эталона для других общих физических каналов нисходящей линии связи. Более того, это рассматривается как чисто физический канал, поскольку он не несет данных. CPICH используется для принятия решений о передаче обслуживания (handover), выборе сот и повторные выборы, и, при некоторых обстоятельствах, чтобы помочь в канале предварительный расчет. Достижение достаточного покрытия CPICH важно, чтобы обеспечить надлежащую функциональность выбора ячеек и повторный выбор, и измерения передачи. Тем не менее, CPICH также потребляет ограниченную мощность передачи из-за того, что базовые станции отправляют свои уникальные CPICH сигналы непрерывно. Следовательно, распределение мощности CPICH является одной из важных задач в планировании сети WCDMA. На практике, однако, покрытие CPICH должно перекрываться в пограничных зонах сот для возможности мягких хэндоверов (SHO) и в для того, чтобы добиться надлежащего внутреннего покрытия на границах ячейки (рис. 1) [1].

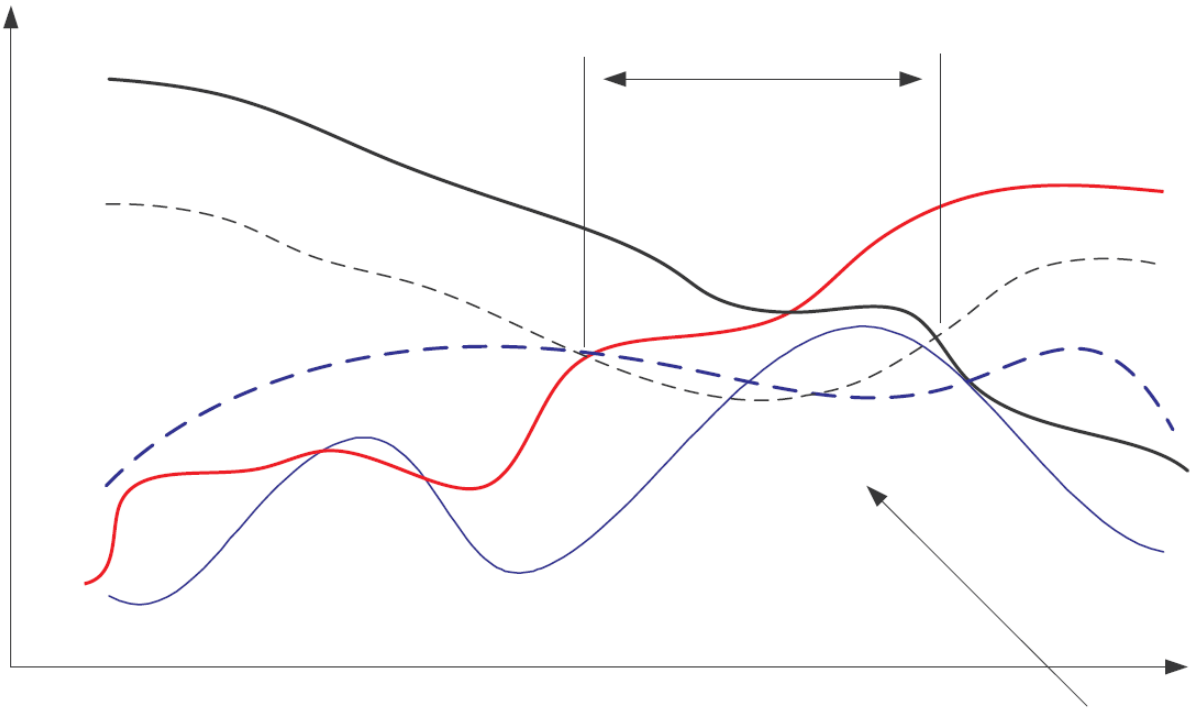


Рис 1. – Пример мягкого хэндовера

Пилотное загрязнение наблюдается в районах, где много сигналов CPICH (разные сигналы CPICH или их многолучевые компоненты), полученные на RAKE приёмник мобильной станции, чем он способен обрабатывать, или ни один из полученных сигналов CPICH достаточно доминирующий [2]. Каждая сота, которую слышит мобильный телефон, практически увеличит уровень помех в нисходящей линии связи (DL). Таким образом, слушая ненужные пилотные сигналы снижается принимаемая энергия на чип по удельной мощности (E_c / N_0) от обслуживающей соты; другими

словами, уменьшает качество существующего соединения. Чтобы избежать пилотно загрязненных участков, зоны доминирования сот должны быть по возможности чистыми и ненужные сигналы CPICH не должны быть услышаны. Тем не менее, пилотного загрязнения нельзя полностью избежать традиционными методами планирования радиосети из-за неоднородной среды распространения и перекрытия сот.

В общем, помехи от пилотного загрязнения могут быть уменьшены оптимизацией мощности пилотного сигнала автоматически таким образом, чтобы требуемые пороги покрытия все еще превышены. Простым методом управления мощностью CPICH, производительность радиоинтерфейса сети WCDMA может быть немного улучшена. Реализация репитеров может также уменьшить помехи от пилотных помех в сетях CDMA. Очевидно, что ретрансляторы способны уменьшить пилотные загрязненные районы сделать область доминирования донорских клеток более четкой, тем самым уменьшая вклад мешающих пилотов. Однако ретрансляторы могли сдвинуть помехи от пилотного загрязнения от доминированной области ретрансляторов, создавая территорию пилотных загрязнений в другом месте.

В этой работе, количество пилотных загрязненных территорий было изучено в сотовой сети WCDMA с разными сценариями секторов, диаграммы направленности антенны, направления и наклон антенны. Результаты показывают, что пилотные загрязненные районы можно уменьшить, выбрав подходящую конфигурацию антенны базовой станции. Диаграмма направленности антенны и направление антенны также имеет явное влияние на пилотное загрязнение. Кроме того, наклон антенны влияет на пилотно загрязненные районы.

Список использованных источников:

1.Дж. Лайхо, А. Вакер, Т. Новосад (ред.), Планирование и оптимизация радиосети для UMTS. Чичестер: John Wiley & Sons Ltd, 2002.

2.Дж. Лемпиайнен, М. Маннинен (ред.), Планирование, оптимизация и управление QoS UMTS радиосети. Дордрехт: Kluwer Academic

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

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

Жлобо М.В.

Королев А.И. – к.т.н., доцент

21-й век демонстрирует исключительно бурное развитие средств связи. Особенно заметны эти изменения в технике и технологии телефонной связи.

Создавая новые сервисные возможности для пользователей, современная техника телефонной связи продолжает оставаться наиболее привлекательной для целей шпионажа, шантажа, устремлений преступных элементов и др.

За достаточно длительный период своего развития человечество накопило огромный опыт и массу знаний о способах и средствах ведения разведки. Естественно, вначале этот опыт носил в основном военный характер, но затем он нашел благодатную почву для “мирной” реализации на ниве промышленного шпионажа. Одним из основных способов ведения разведывательных действий является получение доступа к каналам передачи информации, которыми пользуется конкурирующая сторона. В первую очередь, как правило, нападению подвергаются каналы телефонной связи, по которым, кроме речевой информации, передаются факсимильные, модемные сообщения. Также линии связи с подключенными к ним телефонными аппаратами часто представляют собой нечто вроде “черного хода” в помещение, поскольку большинство телефонных аппаратов ввиду несовершенства конструкции допускают утечку из помещения акустической информации.

В телефонном аппарате (ТА) электрические сигналы распространяются в линиях связи в открытом виде. Практически любой злоумышленник, имея соответствующее оборудование, может получить доступ к конфиденциальной информации, передаваемой в ТА, используя: непосредственное подключение к телефонным линиям связи; бесконтактный съем информации и "жучки"; излучение в радио- и оптическом спектрах частот.

Возможный перечень угроз абоненту показан на рис. 1.

Рис. 1. Перечень угроз абоненту

Все разнообразие технических средств съема информации или их составных частей можно свести к 3-м основным группам:

– средства конспиративного подключения к телефонным линиям и средства передачи информации от них,

– средства коммутации и анализа телефонных каналов,

– средства одноканальной и многоканальной адресной записи телефонных разговоров.

Современные способы защиты телефонных линий можно разбить на две основные группы:

– организационные;
– технические.

Под **организационными способами** понимается комплекс организационно-правовых и организационно - технических мероприятий, проведение которых исключали бы или, по крайней мере сводили к минимуму возможность перехвата телефонных переговоров с линии. Данные способы основаны на ограничении физического доступа к линии и аппаратуре связи и на преобразовании сигналов в линии к форме, исключающей (затрудняющей) для злоумышленника восприятие или искажение содержания передачи.

Под **техническими способами** противодействия понимается применение на телефонных линиях средств анализа и контроля, специальных технических средств защиты

На рис. 2 приведена классификация средств и способов защиты телефонной линии.

Рис.2. Классификация средств и способов защиты телефонной линии

Для организации комплексной защиты информации необходим полный анализ всех возможных угроз, методов и средств защиты, а также экономический анализ целесообразности их применения.

Доступными для обыденного пользователя являются и постановщики активной заградительной помехи. Но, как правило, рекомендуется отказываться от практики постановки помех, ибо ряд современных АТС автоматически определяет стороннее переменное напряжение и отключает абонента от станции.

Наиболее эффективной мерой защиты информации является использование криптографических методов, делающих эту информацию недоступной как при прямом прослушивании телефонного тракта, так и при последующей обработке без знания соответствующих методик и алгоритмов дешифровки.

Список использованных источников:

1. Меньшаков Ю.К. Основы защиты от технических разведок. М.: ИПЦ «Маска», 2017г.
2. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации М.: 2010г.
3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации М.: Машиностроение, 2009г.

КОНТРОЛЬ ПОМЕХОУСТОЙЧИВОСТИ ИНФОКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ ПО ЦЕПЯМ ПИТАНИЯ

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

Кишкурно Т.Ю.

Шатило Н.И. – к.т.н.,доцент

Постоянное воздействие внутренних и внешних помех в электрических сетях общего пользования, возрастающая нагрузка в связи с увеличением числа абонентов и видов подключаемого оборудования приводит к усложнению помеховой ситуации в сетях и повышению требований к аппаратуре в отношении электромагнитной совместимости. В связи с этим, для стабильной работы инфокоммуникационного оборудования необходимо применение устройств защиты от сетевых помех. Для оценки эффективности разработанных мер защиты проводятся тестовые испытания оборудования на воздействие таких помех. Тестирование оборудования на устойчивость к помехам осуществляется с помощью имитаторов помех.

Постоянно возрастающая нагрузка электрических сетей в связи с увеличением числа абонентов и видов подключаемого оборудования приводит к усложнению помеховой ситуации в сетях и повышению требований к аппаратуре в отношении электромагнитной совместимости (ЭМС) по цепям питания [1].

Основными источниками помех в электрических сетях общего пользования являются:

1) аварийные режимы работы высоковольтных сетей электропередач;

2) коммутационные помехи при работе мощного технологического оборудования (электромоторы, аппараты сварки, а также природные явления, такие как гроза).

Энергия сетевых пиков может достигать значений единиц килоджоулей, а энергия разрушения современных интегральных микросхем составляет единицы – сотни микроджоулей, т.е. необходимо ослабление сетевой помехи, доходящей до интегральной микросхемы, на 7–9 порядков, что является сложной задачей.

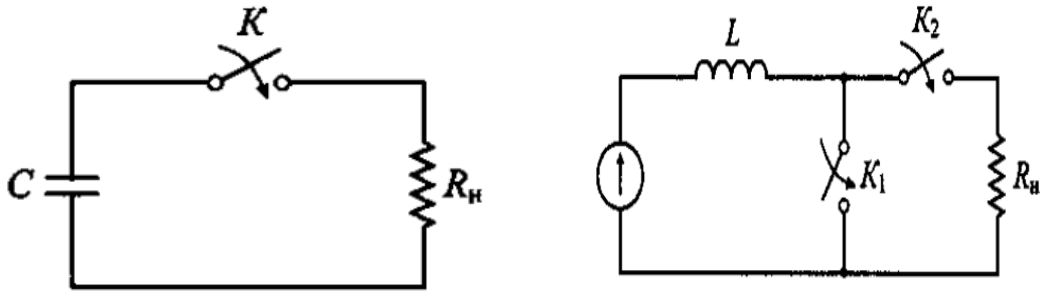
Указанные обстоятельства требуют применения устройств защиты оборудования от сетевых помех. Оценить эффективность разработанных мер защиты позволяют тестовые испытания оборудования на воздействие таких помех. Тестирование оборудования на устойчивость к помехам осуществляется с помощью имитаторов помех. Типовая структура имитатора помех содержит 3 основных компонента:

– накопитель энергии;

– коммутатор;

– формирующая цепь, которая обеспечивает заданные параметры испытательных импульсов.

При формировании импульсов используют накопители в виде катушки индуктивности и в виде конденсатора, показанные на рисунке 1.



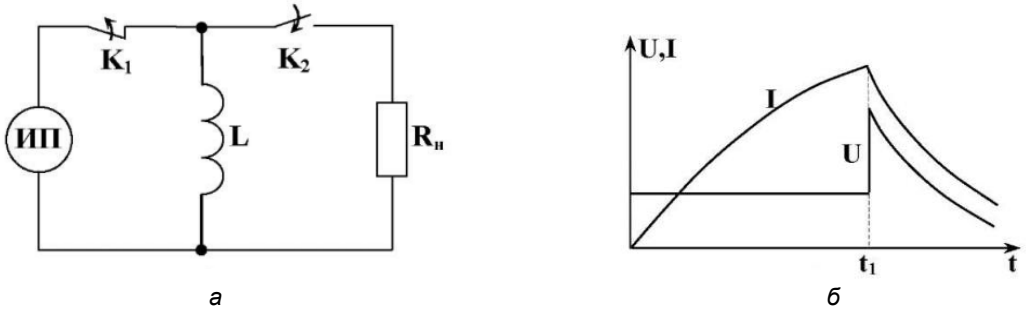
а *б*

Рисунок 1 – Схемы накопителей энергии
а – накопитель в виде конденсатора; б – накопитель в виде катушки индуктивности

Схема простейшего индуктивного накопителя энергии и изменение тока и абсолютного значения напряжения на индуктивности во времени показаны на рисунке 2.

При зарядке до момента t_1 коммутатор K_2 замкнут, от источника питания (ИП) течет нарастающий ток. Напряжение на индуктивности не превышает напряжения источника питания. При достижении необходимого тока (накопления энергии) зарядная цепь размыкается коммутатором K_1, а коммутатором K_2 подсоединяется нагрузка. Накопитель разряжается на нагрузку. При активной постоянной нагрузке ток в ней падает по экспоненте с постоянной времени, определяемой значениями L и R_H. Напряжение на нагрузке, равное напряжению на индуктивности L, в момент коммутации скачком возрастает. При этом мощность, развиваемая в нагрузке, увеличивается по сравнению с мощностью источника питания. Плотность энергии магнитного поля, запасаемой в

индуктивных накопителях, на 2 порядка выше, чем плотность энергии электрического поля, запасаемая в конденсаторах или длинных линиях. Это обстоятельство является решающим при создании накопителей с большими энергиями. При энергиях выше 10^6 Дж индуктивные накопители становятся экономически более выгодными, чем емкостные (например, для термоядерных установок).



а *б*

Рисунок 2 – Схемы индуктивного накопителя энергии
а – схема индуктивного накопителя; б – изменение тока и абсолютного значения напряжения на индуктивности

Индуктивные накопители позволяют получить большую энергию испытательных импульсов, однако амплитуда сформированного импульса существенно зависит от сопротивления нагрузки, т.е. при малой нагрузке это приводит к пробою оборудования, поэтому в имитаторах помех используют емкостные накопители, амплитуда в которых зависит от напряжения заряда конденсатора.

В качестве коммутаторов используют разрядники, тиристоры и транзисторы [2]. Диапазон амплитуды испытательного импульса находится в пределах от 500 до 5000 Вт (согласно ГОСТ) [3]. Эти высокие напряжения требуют применения высоковольтных тиристоров и транзисторов. У высоковольтных транзисторов широкая область коллекторного перехода, что снижает скорость переключения. В то же время допустимое напряжение коллектор-эмиттер составляет 800-1500 В, что ограничивает возможности применения транзисторов в импульсных имитаторах. Те же недостатки характерны и для тиристоров. Необходимость коммутации высокого напряжения так же требует широких p-n переходов, а для больших импульсов тока требуется большая площадь p-n перехода. Эти обстоятельства обуславливают большие значения паразитных емкостей p-n переходов, и, следовательно, малое быстродействие.

Более быстродействующими коммутаторами являются вакуумные разрядники. В имитаторах используются регулируемые и нерегулируемые вакуумные разрядники.

Имитатор импульсов с неуправляемыми вакуумными разрядниками требует включения на выходе частотно-компенсированных высоковольтных аттенюаторов, реализация которых представляет собой сложную техническую задачу. Такая схема реализована в имитаторах, выпускаемых в КБТЭМ объединения «ПЛАНАР». Они используют высоковольтные аттенюаторы фирмы STKEY (США).

Упрощение имитаторов может быть достигнуто при использовании управляемых вакуумных разрядников, включение которых осуществляется с помощью дополнительного электродах [4]. В этом случае пробой не зависит от уровня напряжения на накопителях и легко регулировать амплитуду напряжения, меняя заряд на накопителях. Недостатком таких накопителей является зависимость фронта включения от фронта управляющего сигнала.

Список использованных источников:

1. СТБ МЭК 61000-4-4-2014 Электромагнитная совместимость. Часть 4-4. Методы испытаний и измерений. Испытания на устойчивость к наносекундным импульсным помехам.

2. Черепанов В. П., Хрулев А. К. Тиристоры и их зарубежные аналоги. Справочник. М.: Радиософт, 2002, т.2.

3. ГОСТ Р 51317.4.5 – 12 (МЭК 61000-4-5-11). Совместимость технических средств электромагнитная. Устойчивость к микросекундным импульсным помехам большой энергии. Требования и методы испытаний.

4. Алферов Д. Ф., Иванов В. П., Сидоров В.А. Управляемые вакуумные разрядники и коммутирующие устройства на их основе / Д. Алферов // Мощная импульсная электрофизика. – 2007. №8 – С. 15-17.

БЕЗОПАСНОСТЬ ДАННЫХ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

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

Масько В. С.

Мухуров Н.И. д.т.н.,профессор

Беспроводная сенсорная сеть или беспроводная датчиковая сеть — распределённая, самоорганизующаяся сеть множества датчиков и исполнительных устройств, объединённых между собой посредством радиоканала. Область покрытия подобной сети может составлять от нескольких метров до нескольких километров за счёт способности ретрансляции сообщений от одного узла к другому.

Виды БСС:

- мобильные AD Hoc-сети - Wireless Mobile Ad Hoc Network (MANET);
- беспроводные mash-сети - Wireless Sensor Network (WSN);
- автомобильные беспроводные сети - Vehicular Ad Hoc Network (VANET).

Причины уязвимости безопасности и угрозы в самоорганизующихся сетях:

- каналы уязвимы к прослушиванию и подмене сообщений по причине общей доступности среды передачи, как и в любых беспроводных сетях;
- узлы не защищены от злоумышленника, который может легко изъять их из сети (обычно находятся в открытых местах) и использовать в своих целях;
- отсутствие инфраструктуры делает классические системы безопасности, такие как центры сертификации и центральные серверы, неприменимыми. Динамически изменяющаяся топология сети требует использования сложных алгоритмов маршрутизации, учитывающих вероятность появления некорректной информации от скомпрометированных узлов в результате изменения топологии сети.
- подходы к обеспечению информационной безопасности в мобильных самоорганизующихся сетях значительно отличаются от подходов в реализации ИБ в проводных сетях, ввиду самой природы радиоканала. Связь осуществляется через беспроводную среду, таким образом, передаваемые и получаемые сигналы передаются через воздух. Следовательно, любой узел, находящийся в диапазоне источника сигнала и «знающий» частоту передачи и другие физические параметры (модуляцию, алгоритм кодировки), потенциально может перехватить и раскодировать сигнал, причем ни источник сигнала, ни получатель не будут об этом знать. В проводной сети, наоборот, такой перехват возможен, если злоумышленник физически имеет доступ к проводному каналу, что осуществить гораздо сложнее.

Модель информационной безопасности CIA:

- Конфиденциальность (confidentiality)
- Целостность (integrity)
- Доступность (availability)

Список использованных источников:

1. Бельфер Р. А. Угрозы информационной безопасности в беспроводных саморегулирующихся сетях, 2011
2 Емельяненко И.В. Беспроводные сенсорные сети. Протоколы и технологии // Приоритетные направления развития образования и науки : материалы IV Междунар. науч.–практ. конф. (Чебоксары, 24 дек. 2017 г.) / редкол.: О.Н. Широков [и др.] – Чебоксары: ЦНС «Интерактив плюс», 2017. – С. 177-178. – ISBN 978-5-6040397-8-6.

РОЛЬ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ В ЖИЗНИ СОВРЕМЕННОГО ЧЕЛОВЕКА

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

Нарейко Д.А.

ст. преподаватель Шевчук О.Г.

В 2018 году больше чем две трети из 7,6 млрд мирового населения имеют мобильный телефон, большинство из них являются владельцами смартфонов. За 2018 год число уникальных мобильных пользователей увеличилось более чем на 4 процента. Люди во всем мире предпочитают выходить в интернет со смартфонов. Они генерируют больше веб-трафика, чем все прочие устройства суммарно. Соотношение составляет 53% суммарного трафика с планшетов и смартфонов и 43% с настольных компьютеров. Более того, эти данные относятся только к веб-пользованию. Согласно свежим данным компании App Annie, занимающейся исследованиями рынка мобильных приложений, сегодня люди проводят в мобильных приложениях в 7 раз больше времени, чем в мобильных версиях браузеров. Это говорит о том, что доля мобильных устройств в интернете, вероятнее всего, даже больше вышеуказанной цифры.

Согласно результатам исследований, более 51% цифровых медиа пользователей тратят свое время на загрузку разных типов приложений. В наше время для огромного количества клиентов различных сервисов разработка приложений для смартфонов играет большое значение. Именно с их помощью можно получать возможности пользоваться теми или иными услугами. Мобильные приложения разделяют по нескольким категориям, исходя из того, для какой целевой аудитории оно разрабатывается, какие цели преследует, как будет реализовано. Каждой категории мобильных приложений свойственны свои технические характеристики и особенности реализации. Ниже обозначены основные категории мобильных приложений:

1 Развлечения:

– Игры. Стратегии, гонки, решение головоломок и полеты на кораблях и так далее.

– Заказ билетов в кино, театр, на выставку. Простой и быстрый способ покупки, отзывы и оценки и, соответственно, повышает продажи.

– Приложения для детей. Все, что может заинтересовать ребенка: игры, книги, мультфильмы, музыка, задачки и головоломки и другие развлечения.

– Ночная жизнь и развлечения. Вечеринки, знакомства, танцы, фотографии, видео с мероприятий – все, что может быть интересно активным людям и рекламодателям.

2 Путешествия:

– Заказ отеля и не только. Аренда виллы или машины, заказ номера в отеле и билетов на самолет.

– Туристические гиды. Помогут найти ресторан, магазин или заправку, расскажут интересные факты о достопримечательностях и проложат удобный маршрут.

3 Бизнес:

– Приложения для финансовых организаций и банков. Включают целый ряд профессиональных функций: соотношения валют, индексы, торговые индексы и другое.

– Торговля недвижимостью. Приложения содержат карты с объектами продажи или аренды с подробной информацией о каждом из них.

– Онлайн-продажи. Аукционы, распродажи, коллективные покупки абсолютно любых предметов: от бижутерии до автомобилей.

– Приложения для города. Помогают сориентироваться в мегаполисе, найти нужный объект, проложить маршрут, припарковаться и многое другое.

– Поиск работы. Разместить резюме, просмотреть вакансии, отправить заявки и получить уведомления – обычно такие приложения работают в связке с сайтом.

4 Социальные приложения:

– Социальные сети. Удобны для быстрого общения и обмена информацией, просмотра новостей и уведомлений.

5 Еда:

– Заказ и доставка еды. Приложения, которые позволяют заказывать еду, ставить оценки и оставлять отзывы.

– Определение геолокации заведения.

– Рецепты. Приложения с пошаговыми фото- и видеоинструкциями блюд.

6 Образование:

– Обучение детей. Обучение любым предметам и навыкам в игровой форме.

– Обучение навыкам. ПДД, управление яхтой, дрессировка питомцев или вязание – возможности интерактивных курсов бесконечны.

7 Новости:

– Газеты, журналы и другие СМИ. Такие приложения удобны и значительно расширяют аудиторию изданий. Новости и комментарии могут транслироваться в социальные сети или компилироваться в один RSS-поток.

По итогам 2018 года в каталогах двух самых крупных маркетов, App Store и Play Market, насчитывается более 5 млн приложений, что свидетельствует о востребовательности мобильных приложений в современном мире.

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 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:

1. В. Сердюк. Новое в защите от взлома корпоративных сетей // Техносфера. М. 2007 С.11–63.

ЗАЩИТА ВЕБ-СЕРВИСОВ НА ОСНОВЕ ТЕХНОЛОГИИ WS-SECURITY

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

Михайлов А.С.

Саломатин С.Б. – к.т.н., доцент

Безопасность веб-приложений находится в первой десятке трендов и угроз информационной безопасности уже свыше 10 лет. Тем не менее специализированных средств защиты веб-приложений довольно мало, по большей части эту задачу возлагают (или надеются что она будет решена) на разработчиков. Это и использование различных фреймворков, средств санации, очистки данных, нормализации и многого другого. Со временем усложнялись веб-приложения, серверная инфраструктура и взаимодействие, код становился все более объемным и громоздким — это намного увеличило т.н. "поверхность атаки".

Базы данных

Храните данные идентификации пользователей и конфиденциальные данные (токены, адреса электронной почты, платежные реквизиты) в зашифрованном виде.

Если база данных поддерживает шифрование хранящихся данных (например, AWS Aurora), подключите его для защиты данных на диске. Убедитесь, что все резервные копии также хранятся в зашифрованном виде.

Используйте наименьший уровень привилегий для доступа к учетным записям пользователей в базе данных. Не используйте учётную запись root базы данных.

Предотвращайте SQL-инъекции, используя исключительно подготовленные SQL-запросы. Например: если вы используете NPM, не используйте npm-mysql, используйте npm-mysql2, который поддерживает подготовленные выражения.

Разработка

Убедитесь, что все компоненты приложения проверены на наличие уязвимостей для каждой версии, переданной в продакшн. Сюда входят O/S, библиотеки и пакеты. Проверка должна быть автоматизирована в процессе CI-CD (CI — continuous integration — непрерывная интеграция, CD — continuous delivery — постоянная поставка, прим. перев.).

С одинаковой бдительностью относитесь как к безопасности среды разработки, так и к безопасности сервера. Создавайте программное обеспечение в защищенной изолированной среде разработки.

Идентификация

Убедитесь, что все пароли хэшируются с использованием соответствующей криптографической функции, например, bcrypt. Никогда не пишите собственную функцию хеширования и корректно инициализируйте используемую криптографическую библиотеку случайными данными.

Реализуйте простые, но адекватные правила паролей, которые побуждают пользователей вводить длинные уникальные пароли.

Во всех сервисах используйте многофакторную аутентификацию для входа в систему.

Защита от DDoS-атак

Убедитесь, что DDoS-атаки на ваши API не навредят сайту. Как минимум, защитите «узкие» места API, такие как процедуры генерации логина и токена.

Обеспечьте разумные ограничения по размеру и структуре предоставляемых пользователем данных и запросов.

Смягчайте DDoS-атаки с помощью глобального сервиса с кэширующим прокси, например, CloudFlare. Он включается, когда вы находитесь под DDOS-атакой, а в обычном режиме функционирует как DNS lookup.

Веб-трафик

Используйте TLS для всего сайта, а не только для форм входа и ответов. Никогда не используйте TLS только для формы входа.

Куки должны быть «безопасными» (secure) и httpOnly, а область видимости должна определятся атрибутами path и domain.

API

Убедитесь, что в API нет общедоступных ресурсов.

Убедитесь, что при использовании ваших API пользователи полностью идентифицированы и авторизованы.

Облачная конфигурация

Убедитесь, что все сервисы имеют минимальное количество открытых портов. В то время как принцип «безопасность через неясность» (security through obscurity) не обеспечивает полной защиты, использование нестандартных портов немного усложнит жизнь злоумышленникам.

Размещайте базу бекэнда на частных VPC, которые не видны в публичной сети. Будьте очень осторожны при настройке групп безопасности AWS и пиринговых VPC — можно непреднамеренно сделать службы публичными.

Инфраструктура

Убедитесь, что апгрейды делаются без простоя, а ПО обновляется автоматически.

Не используйте SSH в службах, кроме разве что разовой диагностики. Регулярное использование SSH, как правило, означает, что вы не автоматизировали все как надо.

Эксплуатация

Выключите неиспользуемые службы и серверы. Самый безопасный сервер — это выключенный сервер.

Тестирование

Проводите аудит и проекта, и готовой реализации.

Список использованных источников:

1. Michael O’Brien https://simplesecurity.sensedeep.com/web-developer-security-checklist-f2e4f43c9c56

АЛГОРИТМЫ ОБНАРУЖЕНИЯ ЗАБОЛЕВАНИЙ КОЖИ ПО ИЗОБРАЖЕНИЮ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

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

Медведев Е.А.

Борискевич И.А. – к.т.н.,доцент

В настоящее время в связи с развитием и распростронением нейронных сетей и искусственного интелекта, появляются возможности расширения различных сфер, касающихся жизни общества, к примеру нейронные сети уже обрабатывают фотографии в телефоне, корректируют поисковые запросы под конкретного пользователя, предлагают интересующую его рекламу и т.п. Так же нейронные сети уже достаточно давно умеют распозновать лица людей, что успешно используется в огромном количестве алгоритмов аутентификации. В последнее время появляются разработки в данной области, призванные помочь в здравоохранении, как например распознование кожных заболеваний по изображению.

Искусственная нейронная сеть (ИНС) — математическая модель, а также её программное или аппаратное воплощение, построенная по принципу организации и функционирования биологических нейронных сетей — сетей нервных клеток живого организма. Это понятие возникло при изучении процессов, протекающих в мозге, и при попытке смоделировать эти процессы.

Существует несколько вариантов представления искусственной нейронной сети, таких как: Нейронная сеть с прямым распространением, нейронная сеть с обратным распространением и т.д. На рисунке 1 представлена простейшая модель ИНС с прямым распространением.

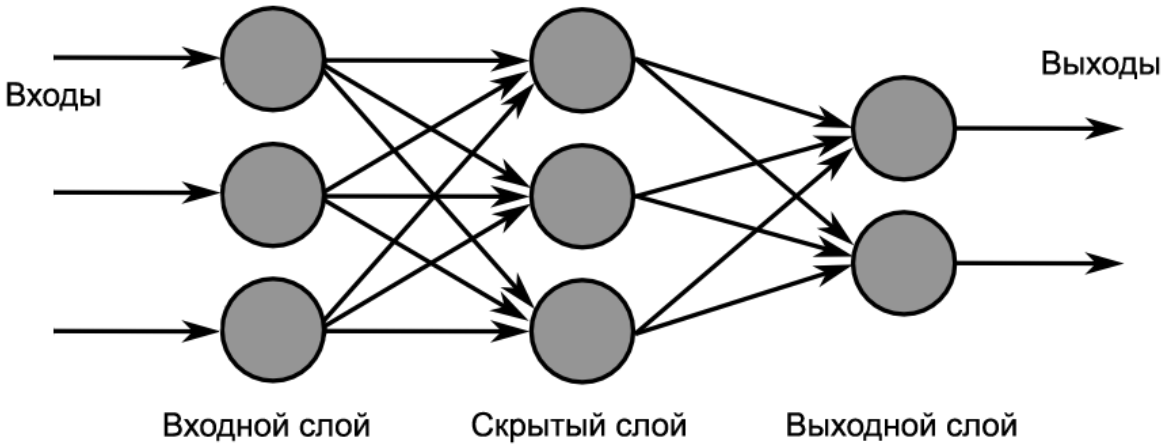


Рис.1 — Простейшая модель нейронной сети.

На схеме мы можем наблюдать входной слой, состоящий из нескольких нейронов, на которые подаются входных данные. Количество нейронов на входном слое зависит от задачи, выполняемой нейронной сетью. За входным слоем следует скрытый слой (таковых может быть несколько), в котором происходит обработка информации, поступивший на входные нейроны и переданной на скрытый слой. Количество нейронов на данном слою так же вариативно и зависит напрямую от задачи, поставленной нейросети, и функции активации, выбранной для конкретной сети. Далее мы можем видеть выходной слой, количество нейронов на котором так же может изменяться в зависимости от задачи и желаемых результатов. Нейроны соединены между собой методом каждый с каждым в рамках соседних слоев. У каждого нейрона есть свой вес (Весовой коэффициент), который формируется в процессе обучения и показывает значимость данного нейрона для общей задачи.

Для построения алгоритма распознавания кожных заболеваний необходимо рассмотреть упрощенную модель кожи, представленную на рисунке 2. Так же для корректной работы алгоритма необходимо при обработке изображения выбрать наиболее подходящее цветовое пространство. Обоснование выбора которого присутствует в работе. Выбор типа нейронной сети, а так же алгоритм ее обучения и функции активации так же важны для любой задачи. Алгоритм обучения нейронной сети — это процесс, в котором параметры нейронной сети настраиваются посредством моделирования среды, в которую эта сеть встроена. Тип обучения определяется способом подстройки параметров. Различают алгоритмы обучения с учителем и без учителя. Функция активации нейронной сети — функция, определяющая выходной сигнал на основании входного сигнала или набора сигналов.

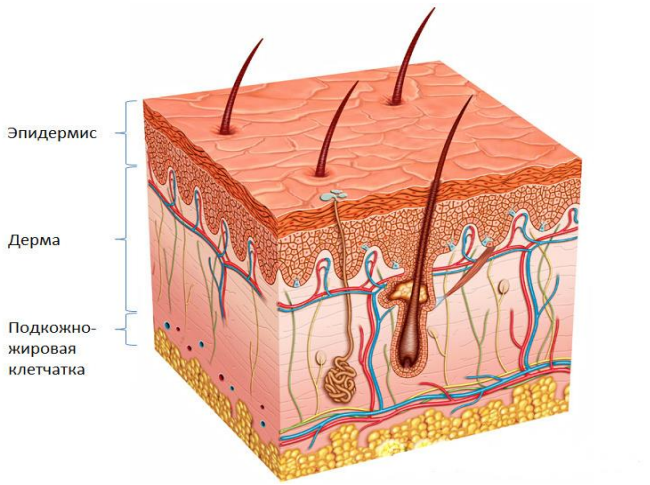


Рис.2 — Упрощенная модель кожи.

Обнаружение кожных заболеваний состоит из следующих этапов:

1. **Получение изображения**. На данном этапе получается изображение;
2. **Предварительная обработка изображения.** На втором этапе производится предварительная обработка использованием медианного фильтра**.** Медианный фильтр используется для удаления нежелательных волос, пузырьков и шума с изображений. Изображение кожных заболеваний обычно содержит тонкие волосы, шум и пузырьки, которые не являются факторами риска и смело могут быть удалены.
3. **Сегментация.** На третьем этапе сегментация выполняется с использованием порогового значения. Изображение порогового значения — это техника для установленных границ изображения, которые содержат твердый объект на контрастном фоне.
4. **Функция извлечения.** На четвертом шаге элементы извлекаются с использованием техники выделения признаков. В методике выделения признаков полезная информация извлекается из сегментированного изображения. Выделение признаков выполняется с использованием многоуровневого выевлет-разложения.
5. **Классификация искусственной нейронной сети.** На пятом этапе эта информация используется в системе классификации для обучения и тестирования. Классификация осуществляется с использованием нейронной сети обратного распространения и радиальной базовой нейронной сети.
6. **Получение предварительного результата.** На последнем шаге находятся данные о кожных заболеваниях.

Список использованных источников:

1 R.G. White and D.A. Perednia, “Automatic Derivation of Initial Match Points for Paired Digital Images of Skin,” Computerized Medical Imaging and Graphics, vol. 16, no. 3, pp. 217-225, 1992.

2 Joao Manuel, R. S. Tavares, M. Natal Jorge, “Computational Vision and Medical Image Processing, Recent Trends”, Vol. 19, pp.145-154, Springer Publication, 2011

3 Sonali Raghunath Jadhav, D.K.Kamat. ”Segmentation based detection of skin cancer” IRF international conference, 20- july-2014

КОДИРОВАНИЕ И ПЕРЕДАЧА ДАННЫХ В СИСТЕМЕ ВИДЕОНАБЛЮДЕНИЯ

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

Чечко А.С.

Мухуров Н.И. – докт. техн. наук, доцент

Понятие цифрового телевидения подразумевает передачу кодированного видеосигнала по цифровому каналу связи. В данном случае под кодированием понимается преобразование сигнала в вид, удобный для передачи по соответствующему каналу связи. Для снижения нагрузки на него при кодировании видеосигнала используется сжатие данных. Кроме того, это позволяет экономить объемы архива при хранении.

Для того, что бы определить размер архива или суммарный объем жестких дисков требуемый для хранения архива системы видеонаблюдения необходимо определится с кодеком сжатия. Именно от него будет зависть размер архива.

Разные кодеки имеют разную степень сжатия информации исходного файла. Основные кодеки применяемые в системах видеонаблюдения: H.264, MJPEG, MPEG4, Motion Wavelet, JPEG2000, MxPEG. Размер будет зависеть от типа используемого кодека. Кодеки можно поделить на два типа:

- покадровые (выполняющие сжатие каждого кадра (*MJPEG, JPEG2000*));
- межкадровые (выполняющие сжатие последовательности изображений (*H.264, MPEG4, Motion Wavelet, MxPEG*)).

Преимущества покадровых перед межкадровыми кодеками заключается в том, что дают четкие кадры без артефактов и предсказательной логики. Любой момент можно четко рассмотреть. Нет зависимости от ключевых кадров.

Преимущества межкадровых – меньший размер кадра, соответственно уменьшение необходимой пропускной способности канала.

Методы сжатия разделяются на две группы - с потерями и без потерь. Первая группа обеспечивает лучший коэффициент сжатия, однако после него исходные данные восстановить невозможно, что выражается в искажениях, потере качества. Сжатие без потерь показывает очень низкую эффективность применительно к графическому контенту.

На данный момент наиболее распространенными стандартами сжатия видео являются H.264 и MJPEG. Важным отличием второго является то, что каждый кадр видео сжимается независимо от других, что гарантирует всегда четкую картинку на стоп-кадре. Помимо этого, MJPEG менее требователен к вычислительным ресурсам, что позволяет удешевлять конструкцию использующих его устройств или достигать недоступного для H.264 быстродействия. Обратной стороной медали является низкий коэффициент сжатия. Так, при средних настройках качества плотность записи для H.264 в 10-20 раз выше, чем для MJPEG.

В настоящее время готовится к внедрению H.265, известный также как HVEC (High Efficiency Video Coding - высокоэффективное видеокодирование). По сравнению с H.265 обеспечивает повышение сжатия более чем на 30%, а при одинаковой степени сжатия - лучшее качество и быстродействие.

Стоит также отметить свободный видеокодек DaaLa, разрабатываемый некоммерческой организацией Xiph.Org Foundation. По своим характеристикам он превосходит H.265 и после окончания разработки может вытеснить его за счет бесплатной лицензии.

Необходимо также сказать несколько слов о медиаконтейнерах - таково обобщенное название форматов файлов с мультимедийным содержанием. Наиболее известными из них являются avi, mov, mp4 (m4v) и mkv. Предназначение медиаконтейнеров в том, чтобы объединять аудио и видео дорожки, субтитры, а также нести сопутствующую информацию - сообщать об используемых кодеках, количестве кадров в секунду и т.п.

Список использованных источников:

1. Крахмалев А.К. Средства и системы контроля и управления доступом. Учебное пособие. М.: НИЦ "Охрана" ГУВО МВД России. 2003.

2. Зайцева Е.В. Классификация современных методов трекинга объектов в интеллектуальных системах видеонаблюдения КТЦ "Охранные системы", 2015.

ВИРТУАЛИЗАЦИЯ СЕРВЕРОВ НА БАЗЕ VMWARE ESXI

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

Картошников Д.Н.

Королев А.И. – к.т.н.,доцент

Быстрое развитие рынка технологий виртуализации за последние несколько лет произошло во многом благодаря увеличению мощностей аппаратного обеспечения, позволившего создавать по-настоящему эффективные платформы виртуализации, как для серверных систем, так и для настольных компьютеров. Технологии виртуализации позволяют запускать на одном физическом компьютере (хосте) несколько виртуальных экземпляров операционных систем (гостевых ОС) в целях обеспечения их независимости от аппаратной платформы и сосредоточения нескольких виртуальных машин на одной физической.

В наши дни виртуализация на платформах Windows принимает одну из двух форм: тип 2 и гибридная (hybrid). Все начинается с базовой ОС, то есть с ОС, которая устанавливается непосредственно на физическое оборудование. Поверх базовой ОС работает монитор виртуальных машин (Virtual Machine Monitor, VMM), в задачу которого входит создание виртуальных машин и управление ими, распределение ресурсов между машинами, обеспечение изоляции машин друг от друга. Иными словами, в данном сценарии VMM играет роль уровня виртуализации (virtualization layer). Затем поверх VMM работают уже гостевые приложения. Ее производительность не велика, поскольку приложениям на пути к оборудованию приходится проходить как через VMM, так и через базовую ОС. [1]

В IT-среде более распространена гибридная виртуализация. Здесь непосредственно с оборудованием общаются как базовая ОС, так и VMM (хотя к различным аппаратным компонентам они имеют разный доступ), а гостевые ОС работают поверх уровня виртуализации. Точее, в этой конфигурации VMM также должен проходить через базовую ОС, чтобы получить доступ к оборудованию. Однако, как базовая ОС, так и VMM работают в режиме ядра и потому, по сути, конкурируют за обладание ресурсами ЦП. Базовой системе циклы процессора выделяются по мере надобности в ее контексте, затем циклы передаются VMM, а VMM передает циклы гостевым ОС. Процесс повторяется снова. Гибридная форма работает быстрее формы типа 2, поскольку в первом случае VMM работает в режиме ядра, а во втором – в пользовательском режиме

Имеется и третий тип технологии виртуализации – VMM типа 1 или технология гипервизора. Гипервизор (hypervisor) – это программный уровень, расположенный непосредственно над оборудованием и под одной или несколькими ОС. Его основное назначение – организовать изолированные среды выполнения, называемые разделами (partition), внутри которых будут работать виртуальные машины с гостевыми ОС. Каждому разделу выделяется собственный набор аппаратных ресурсов, в который входят память, процессорное время и устройства, а гипервизор отвечает за организацию доступа к реальному оборудованию.[2]

Можно сравнить два варианта VMM типа 1: монолитный и микроядерный.

В монолитной (monolithic) модели гипервизор использует для доступа к оборудованию собственные драйверы Гостевые ОС работают на виртуальных машинах поверх гипервизора. Когда гостевой системе нужен доступ к оборудованию, она должна пройти через гипервизор и его модель драйверов. Обычно одна из гостевых ОС играет роль ад-министратора или консоли, в которой запускаются компоненты для предоставления ресурсов, управления и мониторинга всех гостевых ОС, работающих на компьютере. Модель монолитного гипервизора обеспечивает прекрасную производительность, но уязвима с точки зрения защищенности и устойчивости. Это связано с тем, что она по своей сути обладает более широким фронтом нападения и подвергает систему большему потенциальному риску, поскольку разрешает работу драйверов (а иногда даже программ сторонних производителей) в очень чувствительной области.

Альтернативу монолитному подходу составляет микроядерная (microkernelized) модель. В ней можно говорить о «тонком гипервизоре» – в этом случае в нем совсем нет драйверов. Вместо этого драйверы работают в каждом индивидуальном разделе, чтобы любая гостевая ОС имела возможность получить через гипервизор доступ к оборудованию. При такой расстановке сил каждая виртуальная машина занимает совершенно обособленный раздел, что положительно сказывается на защищенности и надежности. Родительский раздел, является также корневым (root), поскольку он создается первым и владеет всеми ресурсами, не принадлежащими гипервизору. Обладание всеми аппаратными ресурсами означает среди прочего, что именно корневой (то есть, родительский) раздел управляет питанием, подключением самонастраивающихся устройств, ведает вопросами аппаратных сбоев и даже управляет загрузкой гипервизора. В родительском разделе содержится стек виртуализации – набор программных компонентов, расположенных поверх гипервизора и совместно с ним обеспечивающих работу виртуальных машин. Стек виртуализации обменивается данными с

гипервизором и выполняет все функции по виртуализации, не поддерживаемые непосредственно гипервизором. Большая часть этих функций связана с созданием дочерних разделов и управлением ими и необходимыми им ресурсами (центральный процессор, память, устройства). Стек виртуализации также обеспечивает доступ к интерфейсу управления.

Преимущество микроядерного подхода, примененного в Windows Server, по сравнению с монолитным подходом состоит в том, что драйверы, которые должны располагаться между родительским разделом и физическим сервером, не требуют внесения никаких изменений в модель драйверов. Иными словами, в системе можно просто применять существующие драйверы. В Microsoft этот подход избрали, поскольку необходимость разработки новых драйверов сильно затормозила бы развитие системы. Что же касается гостевых ОС, они будут работать с эмуляторами или синтетическими устройствами. С другой стороны, микроядерная модель может несколько проигрывать монолитной модели в производительности. Однако главным приоритетом стала безопасность, поэтому для большинства компаний вполне приемлема потеря пары процентов в производительности ради сокращения фронта нападения и повышения устойчивости.[3]

Список использованных источников:

1. Преимущества виртуализации [Электронный ресурс]. – Режим доступа: https://technet.microsoft.com/ru-ru/gg715011
2. Архитектура Hyper-V. Глубокое погружение [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/98580/
3. Михеев, М. Администрирование VMware vSphere 5 / М. Михеев. – СПб.: ДМК Пресс, 2012. – 508 с

ОБРАБОТКА ТЕПЛОВИЗИОННЫХ ИЗОБРАЖЕНИЙ НА МИКРОКОНТРОЛЛЕРЕ RASPBERRY PI

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

Ксендиков В.С.

Кореневский С.А. – к.т.н., доцент

Любые физические объекты (тела) имеют возможность излучать, поглощать, отражать и пропускать инфракрасное (далее – ИК) излучение, если их температура отлична от абсолютного нуля, что даёт возможность извлекать информацию об исследуемом объекте. ИК излучение отличается от видимого и превосходит последнего тем, что оно может проходить сквозь атмосферную дымку, замутненную среду, туманы и полную темноту, позволяя видеть объекты, удаленные на расстояние в десятки и сотни километров[1, 2].

Для визуализации объектов, полученных с помощью ИК излучений, необходимо выполнить предварительную обработку изображения. Под предобработкой понимается применение фильтров улучшения, контрастирование, удаление шумов, применение различных масок, а для выделения объектов и их последующего анализа производится сегментация изображения. Эти операции будут производиться на микроконтроллере Raspberry Pi.

Raspberry Pi является одноплатным компьютером размером чуть большим кредитной карты. На Raspberry Pi 3 установлен 64-х битный четырёхядерный процессор ARM Cortex-A53 с тактовой частотой 1,2 ГГц на ядро в составе однокристальной платформы Broadcom BCM2837, имеет 1 Гб оперативной памяти и интерфейсы коммуникации, такие как Wi-Fi, Bluetooth и Ethernet.

Одна из самых ресурсозатратных операций, которые будут производиться на микроконтроллере - это сегментация изображения, она представляет собой распределение множества пикселей изображения на объекты и области фона, которые отличаются друг от друга по каким-либо признакам, например, цвет, яркость. Один из алгоритмов сегментации – пиксельная сегментация изображения на основе квадродерева, в нём изображение рассматривается как одна область. Если в результате сканирования обнаруживаются несхожие элементы – эта область разбивается на 4 одинаковые по площади подобласти (квадранта) с присвоением каждой из них своего номера. Далее так разбивается каждый квадрант. К найденным при этом смежным однородным квадрантам применяется критерий схожести и если он выполняется – квадранты объединяются в одну область с присвоением одного номера. На рисунке 1 представлен результат разделения изображения на квадранты и соответствующий ему фрагмент квадродерева:

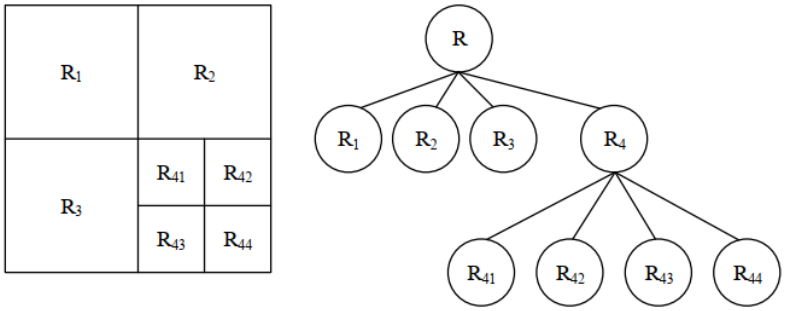


Рис. 1 - Схема сегментации изображения и формирования квадродерева

Согласно рисунку 1 всему изображению соответствует область R (корень квадродерева). На первой итерации обнаруживается неоднородность и данная область разделяется на 4 квадранта R_1, R_2, R_3, R_4 (что приводит к образованию соответствующих четырех узлов в квадродереве). Полученные четыре квадранта обрабатываются на следующей итерации отдельно. В первых трех квадрантах обнаруживается схожесть всех элементов и эти квадранты далее не сегментируются (новые ветви в квадродереве от данных узлов не образуются). В квадранте R4 обнаруживается неоднородность и он дробится на следующей итерации еще на четыре квадранта R_{41}, R_{42}, R_{43}, R_{44} (с образованием новых четырех узлов в квадродереве).

Данный метод сегментации, используя микроконтроллер Raspberry Pi, позволяет повысить точность определения границ на сильно зашумлённых и тепловизионных изображениях с большим количеством перепадов яркостей. Из недостатков можно выделить существование высокой вероятности пересегментации изображений, она проявляется в присвоении различных номеров одной области и приводит к росту числа сегментов.

Список использованных источников:
1. Госсорг Ж. Инфракрасная термография. Основы, техника, применение. — М.: Мир, 1988.
2. Логинов И. Д. Обработка и сегментация тепловизионных изображений // Молодой ученый. — 2017. — №13.

ПРЕИМУЩЕСТВА ПРИМЕНЕНИЯ ТЕОРИИ ПОЛЕЙ ГАЛУА ДЛЯ ОБРАБОТКИ КОДОВ РИДА-СОЛОМОНА

Военная академия Республики Беларусь
г. Минск, Республика Беларусь

Семёнов С.И.

Липницкий В.Н. – д.т.н., профессор

В докладе проведен обзор и критический анализ классических методов обработки кодов Рида-Соломона, установлены достоинства и недостатки этих методов, констатирована необходимость развития матричных методов обработки кодов Рида-Соломона на основе теории полей Галуа.

Цифровые системы передачи играют подавляющую роль в современной информационной эпохе. Инфокоммуникационные системы (ИКС) на их основе обеспечивают надежность и достоверность передачи информации благодаря использованию помехоустойчивого кодирования. Суть его заключается во введении избыточной информации в передаваемую с тем, чтобы в последующем, при передаче закодированного сообщения в каналах с шумами, ИКС могла бороться с возможными возникающими ошибками. Среди многообразия применяемых помехоустойчивых кодов значительную роль играют коды Рида-Соломона (РС-коды) [1–5]. Специфической особенностью РС-кодов является их работа с недвоичным алфавитом. Коды Рида-Соломона были созданы в 1960 году [6], однако только с появлением техники с большими вычислительными ресурсами стало возможным эффективно реализовать на их основе устройства в высокоскоростных цифровых системах передачи и обработки информации реального времени. Они активно применяются в самых различных цифровых системах передачи и обработки данных: в сетях ЭВМ; в оптических системах; при передаче информации в сети WiMax; в спутниковой, радиорелейной связи; в системах хранения данных (RAID 6) и т.д. [1].

Для декодирования ошибок РС-кодами разработана система различных методов: алгоритм Питерсона-Горенстейна-Цирлера, алгоритм Берлекэмпа-Месси, алгоритм Форни [1,2], а также более новые – алгоритм Судана [7] и другие.

Особенно эффективно РС-коды проявили себя при коррекции ошибок весом 1. Однако как показывают проведенные исследования, коррекция ошибок кратностью ω≥2 требует определенной осторожности. Так, например, трехзначная ошибка может быть декодирована как двухзначная при использовании алгоритма декодирования для двухзначной ошибки, и наоборот – двухзначная может быть интерпретирована как трехзначная, что в результате может привести к еще большему искажению принятого сообщения. Поэтому требуется проводить дополнительную проверку на правильность полученного кодового слова, что недопустимо в высокоскоростных системах передачи информации. В этих случаях работа декодера с РС-кодами требует уверенного знания кратности исправляемых ошибок.

Определение РС-кодов близко к определению БЧХ-кодов, для которых разработана теория норм синдромов (ТНС) [8], позволившая эффективно использовать теорию полей Галуа и теорию автоморфизмов кодов для их обработки. На основе ТНС предложен ряд перестановочных норменных методов коррекции ошибок БЧХ-кодами, на порядок снижающих проблемы «селектора», напрямую не зависящих от веса исправляемых ошибок.

Несомненно, развитие ТНС на класс РС-кодов позволит предложить такие же эффективные методы их обработки. Следует заметить, что реализация этой идеи требует последовательного изложения теории РС-кодов на матричном языке с максимальным упором на теорию полей Галуа, роль которой еще недостаточно проявилась в теории и практике РС-кодов, поэтому перенос основных положений ТНС на семейства РС-кодов должны принести новые эффективные методы обработки этих кодов

Список использованных источников:

1. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр : – пер. с англ. – Изд. 2-е, испр. – М. : Вильямс, 2003. – 1104 с.

2. Кудряшов, Б. Д. Основы теории кодирования : учеб. пособие. – СПб. : БХВ-Петербург, 2016. – 400 с.

3. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн : Пер. с англ. – М. : Связь, 1979. – 744 с.

4. Блейхут, Р. Теория и практика кодов, контролирующих ошибки : Пер. с англ. – М. : Мир, 1986. – 576 с.

5. Сидельников, В. М. Теория кодирования. – М. : ФИЗМАТЛИТ, 2008. – 324 с.

6. Reed I. S., Solomon G. Polynomial codes over certain finite fields. Journal of the Society for Industrial & Applied Mathematics, 1960, 8(3). – Pp. 300 – 304.

7. V. Guruswami and M. Sudan, «Improved decoding of Reed-Solomon and algebraic-geometric codes», IEEE Transactions on Information Theory, September 1999, 45(7). – Pp. 1757–1767.

8. Липницкий, В. А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения : монография / В. А. Липницкий, В. К. Конопелько. – Минск : Изд. центр БГУ, 2007 – 239 с.

МИРОВОЙ ОПЫТ ВНЕДРЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ТАМОЖЕННЫХ СЛУЖБАХ

Белорусская государственная академия связи
г. Минск, Республика Беларусь

Базаргелдиев Р.

Карпук А.А. – к.т.н., доцент

Приведен обзор опыта внедрения информационных технологий в таможенных службах различных стран. Рассмотрены подходы с приобретением тиражируемой информационной системы и с разработкой национальной информационной системы. Дана краткая характеристика информационных систем, имеющихся на рынке, и собственных информационных систем отдельных стран.

Использование информационных технологий является неотъемлемой составляющей современной таможенной политики. С одной стороны, это обусловлено необходимостью ускорения производства таможенных операций, с другой – способствует прозрачности совершаемых таможенных операций, что снижает коррупционные риски. В настоящее время в развитых странах, в том числе в большинстве постсоветских стран, наиболее активно применяются таможенные информационные технологии предварительного информирования таможенных органов, электронного декларирования товаров с использованием Интернет и автоматического выпуска товаров.

По ряду причин в Туркменистане темпы внедрения информационных технологий в таможенных службах пока отстают от многих стран. Целью научных исследований автора является разработка предложений по дальнейшему развитию применения информационных технологий в таможенных службах Туркменистана. На первом этапе исследований был проведен анализ мирового опыта внедрения информационных технологий в таможенных службах, результаты которого изложены в настоящей работе.

Исходя из опыта разных стран, можно выделить два подхода к информатизации деятельности таможенных служб. Первый подход состоит в приобретении универсальной тиражируемой информационной системы, разработанной для использования в разных странах. Второй подход состоит в разработке национальной информационной системы, ориентированной на собственную страну. Оба варианта имеют свои достоинства и недостатки. В случае внедрения тиражируемой информационной системы внедряющая таможенная служба сталкивается с проблемами ее настройки и доработки под задачи, стоящие перед таможенной службой, с учетом национального законодательства в сфере таможенного оформления. Преимуществами выбора готовой информационной системы являются сравнительно невысокая стоимость и значительное сокращение сроков от момента постановки задачи об информатизации конкретных таможенных процессов до начала штатной эксплуатации реализующей их информационной системы. Недостатками разработки национальной информационной системы является ее высокая стоимость и длительное время разработки и внедрения. Преимуществами являются максимальное соответствие системы потребностям таможенных служб, возможность постоянного совершенствования и развития системы и ее программного обеспечения.

В странах, решивших использовать в таможенных органах покупную систему, возникает проблема выбора информационной системы, в максимальной степени соответствующей потребностям таможенных органов и требующей минимальных затрат на внедрение и эксплуатацию. В настоящее время на рынке имеется более десятка информационных систем, которые могут быть настроены под различные процессы в сфере управления таможенной деятельностью. Наиболее известными из них являются ASYCUDA, SOFI (SOFIX), TIMS/TRIPS-Customs. Все имеющиеся системы разработаны в соответствии с действующими международными стандартами, требованиями Всемирной таможенной организации и Всемирной торговой организации.

Система ASYCUDA [1, 2] разработана экспертами Конференции ООН по торговле и развитию (ЮНКТАД) в целях упрощения и развития международной торговли посредством сокращения времени таможенного оформления товаров. Система является универсальной и легко настраивается под различные задачи, стоящие перед таможенными органами. Она является многоязычной: функционирует на 25 языках, включая русский. Срок внедрения системы занимает около двух лет. Впервые в эксплуатацию данная система была запущена в странах Экономического сообщества стран Западной Африки (ЭКОВАС).

Система ASYCUDA является самой популярной информационной системой, предложенной к тиражированию. В настоящее время различные версии системы (ASYCUDA World, ASYCUDA++, ASYCUDA Version2) используются таможенными службами в 90 государствах, в том числе в государствах ЕС Румынии, Латвийской Республике, Литовской Республике, Республике Мальта, Эстонской Республике, Словацкой Республике. На пространстве СНГ ее используют таможенные службы Республики Молдова, Республики Армения и Грузии.

Система TIMS/TRIPS-Customs была разработана инвестиционным агентством Великобритании Crown Agents и эксплуатируется с 1995 г. Она внедрена в таможенных службах Республики

Мозамбик, Республики Ангола, Содружества Багамских островов, Каймановых островов (заморская территория Великобритании в Вест-Индии), Ямайки, Федерации Сент-Китс и Невис. Частичное внедрение осуществлено в таможенной службе Республики Болгарии, Латвийской Республики, Республики Косово, Республики Филиппины. Однако в настоящее время информация о системе отсутствует на официальном сайте Crown Agents, что говорит о прекращении внедрения и сопровождения системы.

Система SOFI/SOFIX/SOFIWEB [3] разработана французской таможенной службой и эксплуатируется с 1974 г. Она используется таможенными службами Арабской Республики Египет, Республики Кот-д'Ивуар, Турецкой Республики, Аргентинской Республики, Республики Парагвай, Республики Гондурас, Таити.

Система e-biscus [4] разработана французской компанией Bull S.A. Она применяется в таможенных службах 28 государств, включая 14 таможенных служб государств ЕС. В настоящее время компания Bull S.A. активно сотрудничает с таможенными службами Республики Болгарии, Республики Кипра, Ирландии, Литовской Республики, Республики Мальта, Королевства Марокко, Республики Польша, Румынии и Турецкой Республики.

Система e-biscus позволяет в режиме реального времени отслеживать поставки, обрабатывать декларации, начислять пошлины, налоги, гарантии, контролировать применение мер нетарифного регулирования, определять высокорисковые грузы, ускорять выпуск товаров. Она предусматривает приоритетную обработку информации уполномоченных экономических операторов, анализ базы данных деклараций в целях выявления высокорисковых поставок, выбор субъектов для постаудитных проверок, анализ результатов расследований и проведения постаудитных проверок для уточнения и коррекции критериев риска. Система e-biscus включает модули: манифест, оформление, тарифного и нетарифного регулирования, систему управления рисками, постаудит. Для стран членов ЕС разработаны специальные модули: TARIC, TQM (Tariff Quotas Management), Surveillance и др.

В последнее десятилетие появилось новое направление в использовании информационных технологий – создание электронного торгового сообщества, объединяющего участников внешнеэкономической деятельности, таможенную службу, банки, грузоотправителей, порты, аэропорты, брокеров, контролирующие органы и т.д., которое получило название технология TradeNet. Она позволяет синхронизировать процессы информатизации таможенных служб, иных контролирующих органов, коммерческих организаций. Данная технология применяется в Республике Сингапур (TradeNet), Республике Сенегал (Orbus 2000), Республике Корея (UNI-PASS) [5].

Из изложенного можно сделать выводы, что среди таможенных служб, внедривших покупные информационные системы, нет таможенных служб экономически развитых государств. Как правило, таможенные службы развитых государств разрабатывают собственной информационной системы, что позволяет им иметь полную свободу действий при развитии таможенной информационной системы и дальнейшей ее модернизации.

Таможенная служба США эксплуатирует несколько независимых систем в рамках интегрированной системы ITDS (система данных международной торговли): основной является ACS (автоматизированная коммерческая система), кроме того, функционируют ABI (автоматизированный брокерский интерфейс), ACH (система автоматизированных платежей), AMS (автоматизированная система подачи манифестов), AES (автоматизированная экспортная система) [6]. Таможенные службы Канады используют совокупность систем ACROSS (система поддержки ускоренного выпуска грузов), CADEX (система обмена данными) и RNS (система подтверждения выпуска). Таможенная служба Российской Федерации также пошла по пути создания собственной информационной системы – Единой автоматизированной информационной системы таможенных органов (ЕАИС).

Результаты проведенного анализа мирового опыта внедрения информационных технологий в таможенных службах будут положены в основу предложений по дальнейшему развитию применения информационных технологий в таможенных службах Туркменистана.

Список использованных источников:

1. Годунов, Д. Информационно-технологические решения ЮНКТАД по внедрению «Единого окна» / Д. Годунов. – 4 с. – [Электронный ресурс]. – Режим доступа: http://www.eurasiancommission.org/ru/act/dmi/inftech/docs_pr/conf/Documents/v8.pdf – Дата доступа: 28.02.2019.

2. О проекте АСИКУДА. – [Электронный ресурс]. – Режим доступа: https://asycuda.org/ru/about-ru/ – Дата доступа: 28.02.2019.

3. Степанова, Е.А. Система таможенного оформления SOFIX / Е.А. Степанова, П.Н. Афонин. – 3 с. – [Электронный ресурс]. – Режим доступа: http://spbrta.customs.ru/spbrta/images/stories/chtenia/2009/PDF/stepanova.pdf– Дата доступа: 28.02.2019.

4. Ермакова, В.В. Использование опыта применения информационных таможенных технологий Европейского Союза при осуществлении таможенного оформления и контроля в Российской Федерации / В.В. Ермакова // Ученые записки Санкт-Петербургского филиала РТА. – 2004. – № 2 (22).– С. 135-139.

5. Кротов, И.Е. Об опыте внедрения информационных таможенных систем в Республике Корея / И.Е. Кротов, В.В. Ермакова // Вестник Российской таможенной академии. – 2010. – № 3.– С. 24-30.

6. Турдубеков, Б.М. Опыт работы таможенных служб промышленно развитых стран / Б.М. Турдубеков, А.Б. Карбекова // ЖАМУнун Жарчысы. – 2015. – № 2.– С. 110-113.

ВНЕДРЕНИЕ КОНЦЕПЦИИ «ИНТЕРНЕТ ВЕЩЕЙ» В СФЕРУ ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА

Белорусская государственная академия связи,
г. Минск, Республика Беларусь

Босак А.В.

Карпук А.А. – к.т.н., доцент

Рассматриваются вопросы внедрения концепции «Интернет вещей» в сферу жилищно-коммунального хозяйства. Предложены варианты реализации умного сбора и контроля показаний счетчиков учета энергоресурсов и умного вывоза отходов из жилых районов.

Жилищно-коммунальное хозяйство (ЖКХ) – важнейшая многоотраслевая социально-экономическая сфера деятельности, целью которой является обеспечение комфортных условий для проживания граждан и создание благоприятной среды обитания. В сферу ЖКХ включены жилищное хозяйство, водоснабжение и водоотведение, теплоэнергетика, обращение с твердыми коммунальными отходами, благоустройство, санитарная очистка и озеленение населенных пунктов. Элементами ЖКХ, куда можно внедрить «Интернет вещей» являются умный сбор и контроль показаний счетчиков учета энергоресурсов и умный вывоз отходов из жилых районов [1].

Для организации умного сбора показаний счетчиков учета энергоресурсов можно использовать специальные счетчики, которые оснащены модулями беспроводной связи и датчиками, способными считывать показания счетчиков. Для работы датчики оснащены батареями с зарядом, способным поддерживать автономную работу на протяжении нескольких лет. Подобное решение позволяет в режиме реального времени рассчитывать стоимость оплаты за тот или иной ресурс, используя данные со счетчиков, которые могут считываться как по запросу, так и через определенный интервал. Кроме дистанционного сбора информации со счетчиков, такая система позволяет дистанционно контролировать подачу ресурсов клиенту [2].

Существует несколько способов реализации данной системы:

- данные можно передавать через сеть мобильного оператора. Для этого счетчики должны быть оснащены модулями передачи через сеть мобильного оператора. Достоинством такого подхода является повсеместная доступность мобильной сети. Главными недостатками такого подхода являются повышенное потребление электроэнергии и использование сети мобильного оператора, что потребует дополнительных денежных средств;
- для многоэтажной застройки данные можно агрегировать на специальном устройстве, которое может размещаться либо во дворе, собирая информацию сразу с нескольких домов, либо на этаже, собирая и данные с датчиков одного этажа;
- можно реализовать передачу данных через модем, который установлен практически в каждом доме. Для этого необходимо использовать специальное устройство, контроллер, которое будет агрегировать данные, поступающие с датчиков, управлять работой сети и преобразовывать информацию из внутреннего протокола сети в вид, необходимый для передачи по сети Интернет.

Кроме умного сбора показаний счетчиков, «Интернет вещей» можно интегрировать в процесс сбора отходов из жилых районов. Для этого требуется установить на контейнеры специальное устройство, считывающее и передающее данные о наполненности контейнеров с помощью встроенных GPS и GPRS-модулей. Для поддержания автономной работы датчиков устройство может быть укомплектовано солнечной батареей.

Использование подобной системы позволяет строить оптимальный план-маршрут по сбору отходов, накапливать статистику за большие периоды времени и предугадывать, когда те или иные контейнеры заполнятся до отказа, строя таким образом графики сбора мусора заблаговременно [3].

Перечисленные способы повышения качества ЖКУ, эффективности использования жилищного фонда и инфраструктуры ЖКХ лягут в основу совершенствования информационных систем, обеспечивающих предоставление комплексной информации об оказании ЖКУ.

Список использованных источников:

1. Умное ЖКХ – [Электронный ресурс] – Режим доступа: https://iot.ru/wiki/umnoe-zhkkh. – Дата доступа: 09.02.2019.
2. Интернет вещей в ЖКХ – [Электронный ресурс] – Режим доступа: https://moydom.media/gkh/internet-veshchey-v-zhkh-3040. – Дата доступа: 17.02.2019.
3. Уборка мусора по-умному – [Электронный ресурс] – Режим доступа: https://iot.ru/gorodskaya-sreda/uborka-musora-po-umnomu. – Дата доступа: 14.02.2019.

СИСТЕМЫ МЕЖВЕДОМСТВЕННОГО ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ В СТРАНАХ ЕВРАЗИЙСКОГО ЭКОНОМИЧЕСКОГО СОЮЗА

Белорусская государственная академия связи
г. Минск, Республика Беларусь

Елыев Б.А.

Карпук А.А. – к.т.н., доцент

Проведен анализ систем межведомственного электронного взаимодействия, используемых в странах Евразийского Экономического Союза. Перечислены основные системы межведомственного электронного взаимодействия и приведены их возможности и характеристики.

Важнейшей подсистемой электронного правительства является система межведомственного электронного взаимодействия, через которую органы власти и государственного управления обмениваются данными, необходимыми для оказания государственных услуг организациям и гражданам. По ряду причин в Туркменистане система межведомственного электронного взаимодействия пока находится на более низком уровне. Целью научных исследований автора является разработка предложений по развитию системы межведомственного электронного взаимодействия в Туркменистане. На первом этапе исследований был проведен анализ систем межведомственного электронного взаимодействия в странах Евразийского Экономического Союза (ЕЭС), результаты которого изложены в настоящей работе.

В зависимости от используемого способа обработки и передачи документов (информационных сообщений) можно выделить следующие технологически различные режимы информационного взаимодействия [1]:

– традиционный бумажный документооборот между сотрудниками организаций, участвующих в межведомственном информационном взаимодействии;

– обмен электронными представлениями (образами) традиционного бумажного документа с использованием доступных электронных технологий информационного взаимодействия – электронная почта, системы электронного документооборота и т.д.;

– унифицированное информационное взаимодействие между информационными системами участников электронного взаимодействия;

– использование интерактивных запросных приложений, предоставляемых некоторыми органами власти и государственного управления в качестве пользовательских электронных сервисов через ведомственные информационные порталы или официальные сайты органов в сети Интернет.

Очевидно, что в рамках электронного правительства должны быть реализованы режимы унифицированного информационного взаимодействия и интерактивных запросных приложений. При этом системы межведомственного электронного взаимодействия должны обеспечить функционирование механизма «единого окна» при проведении внешнеторговых операций [2].

В состав ЕЭС входят Республика Беларусь, Республика Казахстан, Кыргызская Республика и Российская Федерация. В Республике Беларусь для обмена сведениями в электронном виде между государственными органами используются следующие системы [3]:

– система межведомственного документооборота (СМДО);

– общегосударственная автоматизированная информационная система (ОАИС);

– система защищенной электронной почты государственных органов и организаций (СЗЭП Mailgov);

– единая информационная система контроля за поручениями Главы Государства (ЕИС КВП).

СМДО предназначена для автоматизации документооборота между территориально распределенными организациями и их взаимодействия друг с другом посредством ведомственных систем электронного документооборота.

ОАИС обеспечивает предоставление электронных услуг из государственных информационных ресурсов, при этом на Едином портале электронных услуг portal.gov.by предоставляются услуги, не требующие строгой идентификации, а на интранет-портале ОАИС oais.by, доступном только в рамках выделенной сети передачи данных, предоставляются услуги, требующие строгой идентификации.

Основной задачей СЗЭП Mailgov является обеспечение защищенного автоматизированного обмена конфиденциальной информацией, не содержащей сведений, составляющих государственную тайну, между органами государственного управления Республики Беларусь, государственными и иными организациями и предприятиями Республики Беларусь с использованием электронной цифровой подписи (ЭЦП). ЕИС КВП предназначена для автоматизации процесса межведомственного контроля за выполнением поручений Президента страны.

В Республике Казахстан для осуществления обмена сведениями в электронном виде между государственными органами используются следующие системы [4]:

– система межведомственного документооборота (СМДО);

– информационная система «Интегрированное хранилище данных» (ИС ИХД);

– прикладное программное обеспечение Таможенной автоматизированной информационной системы второй очереди (ППО ТАИС-2).

В Кыргызской Республике для осуществления обмена сведениями в электронном виде между государственными органами используется система Tulpar System, предназначенная для выдачи разрешительных документов в сфере внешней торговли [5].

В Российской Федерации для осуществления обмена сведениями в электронном виде между государственными органами используются следующие системы [1]:

– система межведомственного документооборота (СМДО);

– система межведомственного электронного взаимодействия (СМЭВ);

– государственная автоматизированная информационная система «Внешнеторговая информация» (ГАИС «Внешнеторговая информация»);

– система электронного документооборота Минобрнауки России (СЭДО Минобрнауки России);

– ряд ведомственных систем Министерства внутренних дел, Министерства промышленности и торговли и других министерств.

По результатам анализа систем межведомственного электронного взаимодействия в странах ЕЭС можно сделать следующие выводы.

3) Для осуществления межведомственного взаимодействия в Республике Беларусь используются разнородные механизмы с ограничениями совместимости между собой: электронная почта, файловый обмен, веб-сервисы. В качестве основного способа межведомственного взаимодействия используется электронная почта. В Республики Беларусь не используется единая система нормативно-справочной информации (НСИ), при осуществлении процедур межведомственного взаимодействия в основном используется локальная НСИ. Для подписания документов (СМДО), для идентификации пользователя (ОАИС), для подписания и шифрования сообщений и документов (СЭП Mailgov, ЕИС КВП) в Республике Беларусь используются механизмы ЭЦП.

4) В Республике Казахстан практически все системы, за исключением ИС ИХД используют обмен данными посредством сервисов. ППО ТАИС-2 и ШЭП реализуют как взаимодействие посредством HTTP(S), так и взаимодействие через очереди сообщений. Обе системы обмениваются сообщениями на языке XML, в ШЭП реализован также обмен данными в формате PDF. ШЭП использует ЭЦП при передаче документов. При обмене данными через ШЭП используется единая НСИ.

5) Используемая в Кыргызской Республике система Tulpar System не является полнофункциональной системой межведомственного обмена, а представляет собой систему, решающую конкретную прикладную задачу выдачи разрешительных документов.

6) В Российской Федерации все системы, за исключением СМЭВ, не являются полнофункциональными системами межведомственного обмена, а представляют собой ведомственные системы, решающие прикладные задачи в рамках полномочий государственных органов исполнительной власти, отвечающих за функционирование и развитие этих систем. Все системы обмениваются сообщениями в формате XML. СМЭВ использует для обмена инфраструктуру очередей сообщений, почти все остальные системы осуществляют электронный обмен посредством HTTP, HTTP(S). Во всех системах, кроме СЭДО Минобрнауки России, используется механизм ЭЦП. При реализации информационного взаимодействия посредством СМЭВ используется Федеральная единая система НСИ (ФГИС ЕСНСИ).

Перечисленные выводы будут положены в основу предложений по развитию системы межведомственного электронного взаимодействия в Туркменистане, в которой будут реализованы лучшие решения из опыта разработки систем межведомственного электронного взаимодействия в странах ЕЭС.

Список использованных источников:

1. Сенченко, П.В. Способы организации межведомственного информационного взаимодействия / П.В. Сенченко, И.В. Лазарев // Доклады ТУСУР. – 2014. – № 1 (31). – С. 205-208.

2. Бондаренко, А.В. Подходы к созданию механизма «единого окна» в Европейском союзе / А.В. Бондаренко, С.О. Петров // Вопросы инновационной экономики. – 2017. – Том 7. – № 2. – С. 151-160.

3. Электронное правительство в Республике Беларусь: 2017 / ОАЦ при Президенте Республики Беларусь, НЦЭУ. – Минск, 2017. – 31 с. – [Электронный ресурс]. – Режим доступа: https://nces.by/wp-content/uploads/ЭП_финал_просмотр.pdf. – Дата доступа: 28.01.2019.

4. Электронное правительство Республики Казахстан. – [Электронный ресурс]. – Режим доступа: https://egov.kz/cms/ru/information/about/help-elektronnoe-pravitelstvo. – Дата доступа: 28.01.2019.

5. В Кыргызстане «Tulpar System» набирает обороты. – [Электронный ресурс]. – Режим доступа: http://old.kabar.kg/economics/full/50433. – Дата доступа: 28.02.2019.

МИРОВОЙ ОПЫТ ИСПОЛЬЗОВАНИЯ ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Белорусская государственная академия связи
г. Минск, Республика Беларусь

Худайбердиев Р.Г.

Карпук А.А. – к.т.н., доцент

Приведен обзор опыта использования дистанционных образовательных технологий в различных странах. Рассмотрены особенности корреспондентской и трансляционной моделей организации дистанционного обучения. Перечислены используемые технологии и программные средства дистанционного обучения.

Одной из пар виртуального взаимодействия электронного правительства является пара С2К – взаимодействие граждан с учреждениями образования, науки, технологий и инноваций. В соответствии с Законом Туркменистана «Об образовании» образовательные учреждения должны использовать различные образовательные технологии, в том числе дистанционное образование, реализуемое с применением информационно-телекоммуникационных сетей в удаленном режиме. По ряду причин в Туркменистане пока наблюдается отставание уровня дистанционных образовательных технологий от уровня других стран мира. Целью научных исследований автора является разработка предложений по дальнейшему развитию дистанционных образовательных технологий в Туркменистане на основе мирового опыта. На первом этапе исследований был проведен анализ мирового опыта использования дистанционных образовательных технологий, результаты которого изложены в настоящей работе. Анализ проводился на основе данных, приведенных в работах [1-4].

Дистанционное обучение – это обучение в специализированной образовательной среде, включающей электронные учебники и обучающие программы, систему тестирования и контроля знаний, средства обмена информацией и общения с преподавателем и другими участниками учебного процесса. В процессе обучения обучаемый получает доступ со своего компьютера ко всем учебным материалам. Как любая система обучения, дистанционное обучение имеет тот же компонентный состав: цели, содержание, методы, организационные формы и средства обучения. Последние три компонента в дистанционном обучении имеют особую технологическую основу. Информационно-образовательная среда дистанционного обучения представляет собой системно-организованную совокупность средств передачи данных информационных ресурсов, протоколов взаимодействия, программного и организационно-методического обеспечения и ориентируется на удовлетворение образовательных потребностей пользователей.

Дистанционное обучение отличается от традиционного обучения:

– пространственным разделением обучающего и обучаемого;

– усилением активной роли обучаемого в образовательном процессе, предоставлением ему возможности определения целей, выбора форм и темпов обучения;

– подбором учебных материалов, предназначенных специально для дистанционного обучения;

– возможностью обучаться в удобное время в удобном месте и темпе, нерегламентированностью отрезка времени для изучения каждой дисциплины;

– возможностью формировать учебный план из независимых учебных курсов-модулей;

– обучением без отрыва от производства;

– возможностью одновременного обращения ко многим источникам информации;

– эффективным использованием учебных площадей, технических и транспортных средств;

– использованием в образовательном процессе новейших достижений информационных и телекоммуникационных технологий;

– расширением и обновлением роли преподавателя.

Одной из первых стран, внедривших подходы дистанционного обучения, являются США. В середине 60-х годов некоторые американские колледжи начали использовать телевидение для предоставления учебных курсов сотрудникам ближайших фирм. В 1984 г. на базе этих колледжей был образован Национальный технологический университет (NTU). К 1991 г. NTU превратился в консорциум из 40 университетских инженерных школ, в котором более 1100 студентов изучали дистанционным методом программы NTU на инженерную степень при активном участии фирм-работодателей. Для проведения курсов использовались средства, предоставляемые фирмами-работодателями, что является примером кооперации правительственных, университетских и коммерческих структур.

В настоящее время кроме NTU в Северной Америке работают Международный университет Джонса в США (основан в 1993 г., ежегодно обучаются более 30000 человек), Канадский открытый университет в Канаде (основан в 1972 г., ежегодно обучаются более 24000 человек).

В Европе дистанционное образование, в основном, развивается открытыми университетами, которые финансируются правительствами. Наиболее известными являются Открытый университет Великобритании (основан в 1969 г., ежегодно обучаются около 200000 человек), Национальный

университет дистанционного образования в Испании (основан в 1972 г., ежегодно обучаются более 130000 человек), Ферн-Хаген университет в Германии (основан в 1974 г., ежегодно обучаются более 55000 человек), Голландский открытый университет (основан в 1984 г., ежегодно обучаются более 21000 человек).

В Австралии дистанционное обучение проводят Монаш университет (основан в 1961 г., ежегодно обучаются более 49000 человек) и Агентство по открытому обучению (основано в 1992 г., ежегодно обучаются более 14000 человек).

В Российской Федерации лидерами в области дистанционного обучения являются Томский государственный университет управления и радиоэлектроники, Тюменский государственный университет, Московский институт менеджмента, экономики и права, Московский технологический институт. Также можно отметить Московский государственный университет экономики, статистики и информатики, Российский новый университет, Московский индустриальный университет. Кроме того, на территории России работают около 100 иностранных образовательных учреждений с помощью российских посредников.

Показательно, что в странах Ближнего Востока и Центральной Америки, где уровень образования населения и техническая оснащенность образовательного процесса существенно ниже, развитие дистанционного обучения заметно отстает в отличие от других регионов. Переход к новым образовательным технологиям происходит только после достижения некоторого уровня общей и информационной культуры общества при наличии достаточного технического оснащения учебных заведений и населения в целом.

В дистанционном образовании традиционно использовались две модели организации учебного процесса: корреспондентская и трансляционная. В корреспондентской модели дистанционного обучения основной объем аудиторных занятий (лекций и семинаров) не воспроизводится с помощью средств телекоммуникации или аудио и видеозаписи, а заменяется другими интерактивными формами: самостоятельной работой студентов, для организации и обеспечения которой готовятся специальные учебно-методические комплексы, и интенсивными групповыми практическими занятиями. Современная трактовка корреспондентской модели дистанционного образования носит название «британской», поскольку ее основные принципы были разработаны Открытым университетом Великобритании.

В трансляционной модели дистанционного обучения обучение обеспечивается трансляцией на расстояние с помощью современных средств телекоммуникации традиционных очных занятий, что позволяет в десятки или сотни раз увеличить вместимость учебных классов и аудиторий.

В состав технологий дистанционного образования должны входить специальные средства обучения: электронные мультимедийные учебники; мультимедиа-лекции и виртуальные лабораторные практикумы; компьютерные обучающие и тестирующие системы; видео лекции и ряд других обучающих ресурсов. Организационными формами обучения могут быть: групповые консультации в режиме теле видео конференции с удаленной аудиторией; индивидуальные консультации и тесты с использованием телекоммуникационных средств в режимах онлайн и офлайн; лекции вживую для распределенной удаленной аудитории в режиме теле видео конференции; телекоммуникационные трансляции видео лекций в режиме офлайн для распределенных групп обучающихся; консультационные практикумы в режиме теле видео конференций перед выполнением виртуальных лабораторных работ.

В настоящее время имеется большое число различных программных оболочек для организации дистанционного обучения. Это системы управления различными направлениями деятельности вузов, обучающие программы, мультимедиа курсы и т. д. К числу наиболее известных систем вузовского уровня, используемых в Российской Федерации, можно отнести системы «Прометей», «Аванта», ОРОКС, WebCT, Learning Space, MOODLE.

Результаты проведенного анализа мирового опыта использования дистанционных образовательных технологий будут положены в основу предложений по дальнейшему развитию дистанционных образовательных технологий в Туркменистане.

Список использованных источников:

1. Вознесенская, Е.В. Дистанционное обучение – история развития и современные тенденции в образовательном пространстве / Е.В. Вознесенская // Наука и школа. – 2017. – № 1. – С. 116-123.

2. Методические рекомендации по реализации образовательных технологий с применением электросвязи/ИКТ // МСЭ. – 2016. – 44 с. – [Электронный ресурс]. – Режим доступа: https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/Regional%20Initiatives/RI3%20ICT%20in%20education/Recommendations%20on%20implementing%20ICT%20in%20education.pdf. – Дата доступа: 28.01.2019.

3. Юлдашев, З.Ю. Инновационные методы обучения: Особенности дистанционного метода обучения и способы его применения: Учеб. пособие / З.Ю. Юлдашев, Ш.И. Бобохужаев. – Ташкент: IQTISOD-MOLIYA. – 2006. – 180 с.

4. Бочков, В.Е. Состояние, тенденции, проблемы и роль дистанционного обучения в трансграничном образовании: Учеб. пособие / В.Е. Бочков, Г.А. Краснова, В.М. Филиппов. – М.: РУДН. – 2008. – 405 с.

МИРОВОЙ ОПЫТ ВНЕДРЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ГОСУДАРСТВЕННОЕ УПРАВЛЕНИЕ

Белорусская государственная академия связи
г. Минск, Республика Беларусь

Чарыева Э.Е.

Карпук А.А. – к.т.н., доцент

Приведен обзор опыта внедрения информационных технологий в государственное управление в различных странах. Особое внимание уделено странам, занимающим лидирующие позиции по индексу ООН по развитию электронного правительства: Дании, Австралии, Южной Корее, Великобритании.

В последние годы правительства большинства стран мира начали интенсивно использовать информационные и информационно-коммуникационные технологии с целью повышения эффективности и качества своих услуг. Мировой опыт показывает, что внедрение информационных технологий (технологий электронного правительства) предоставляет бизнесу и гражданам доступ к высококачественным услугам государственных органов и одновременно уменьшает стоимость этих услуг.

В настоящее время не существует единой стратегии или шаблона внедрения информационных технологий в государственное управление и формирования и развития электронного правительства. В различных странах внедрение информационных технологий производится по своим принципам. По ряду причин в Туркменистане темпы внедрения информационных технологий в государственное управление пока отстают от многих стран. Целью научных исследований автора является разработка предложений по дальнейшему развитию применения информационных технологий в государственном управлении Туркменистана. На первом этапе исследований был проведен анализ мирового опыта внедрения информационных технологий в государственное управление, результаты которого изложены в настоящей работе.

Концепция e-government (в русском переводе – «электронное правительство») появилась конце 1990-х годов как идея широкого внедрения современных информационных, компьютерных технологий в работу государственных структур с целью повышения эффективности работы государственного аппарата. Первыми странами, в которых была реализована концепция повышения эффективности работы органов государственного управления на основе внедрения электронного правительства, были США, Великобритания, Норвегия и Австралия.

В рамках электронного правительства выделяют несколько модулей взаимодействия, к основным из них относятся [1]:

– пространственным разделением обучающего и обучаемого;
– между различными ветвями государственной власти (G2G);
– между правительством и населением (G2C);
– между правительством и бизнесом (G2B)
– между правительством и общественными организациями (G2N).

По материалам ООН процесс построения электронного правительства в стране состоит из пяти этапов:

1) начальный этап присутствия государства в Интернете, характеризуется наличием официальных правительственных сайтов, предоставляющих информацию в одностороннем порядке;

2) усиленное присутствие государства в Интернете, динамичное предоставление информации с заполнением поисковых форм и элементами взаимодействия с пользователями;

3) интерактивное присутствие государства в Интернете с двусторонним обменом информацией между пользователем и государственными органами, предоставление некоторых онлайн-сервисов и возможности заполнения заявлений в режиме онлайн;

4) присутствие государства в Интернете на уровне транзакций, предоставление пользователям доступа к данным на уровне всех потребностей взаимодействия с государственными органами с возможностью отслеживания рассмотрения своих заявлений в режиме онлайн, реализация транзакций в режиме онлайн (оплата налогов, оплата различных сборов, пошлин, штрафов);

5) полностью интегрированное присутствие государства в Интернете, характеризуется объединением всех государственных Интернет-ресурсов в единый портал государственных услуг.

ООН определяет степень продвижения стран к электронному правительству с помощью индекса развития электронного правительства (e-Government Development Index, EGDI), который является составным индикатором, измеряющим готовность и способность правительства использовать информационно-коммуникационные технологии в целях оказания услуг населению. По результатам оценки в 2018 г. на первом месте по индексу EGDI из 193 стран оказалась Дания, которая в 2016 г. занимала только девятое место [2]. Сохранили свои позиции по отношению к 2016 г. Австралия и Южная Корея, которые занимают второе третье место соответственно. В десятку лучших

стран также вошли Великобритания, Швеция, Финляндия, Сингапур, Новая Зеландия, Франция и Япония. Российская Федерация занимает 32 место, Республика Беларусь – 38 место, Казахстан – 39 место. К сожалению, Туркменистан пока расположился на 147 месте.

С 2016 г. в Дании реализуется «Стратегия в области цифровизации на 2016 – 2020 г.» [3], которая определяет направление проектов по цифровизации государственного сектора Дании, а также вектор взаимодействия с коммерческими организациями и промышленностью. Данная стратегия направлена на закладку основ для надёжной и защищённой цифровизации Дании. Кроме того, в Дании цифровое взаимодействие граждан с государством признано обязательным, но не в ущерб тем, кто не может пользоваться цифровыми услугами. Вместе с частным сектором государственные учреждения местного, регионального и центрального уровня пользуются возможностями, которые даёт цифровизация.

Австралия в 2018 г. осталась на втором месте, которое заняла в 2016 г. Австралия является лидером в сфере развития человеческого капитала и одним из 10 лидеров в сфере онлайн-обслуживания. Правительство Австралии работает над реализацией «Программы цифровой трансформации». Дорожная карта цифровой трансформации, опубликованная в ноябре 2016 г., задаёт цели Программы и фиксирует ожидаемые результаты, которые постоянно актуализируются.

Южная Корея остаётся на третьем месте с 2016 г. Эта страна демонстрирует хорошие показатели в сферах онлайн-обслуживания и технологической инфраструктуры, однако показатель развития человеческого капитала здесь ниже, чем в других странах. В этой стране обеспечено удобное, эффективное и прозрачное взаимодействие с государством, которое обеспечивает рост удовлетворенности граждан и продуктивности государственного управления, а также постоянно совершенствуется для повышения уровня оказания услуг на фоне быстрых технологических изменений.

Великобритания занимает четвёртое место по результатам 2018 г. Страна потеряла первенство, которого добилась по результатам 2016 г. Снижение позиции обусловлено относительным снижением рейтинга человеческого капитала и индекса онлайн-обслуживания. Правительство Великобритании оказывает комплексные онлайн-услуги при помощи платформы gov.uk, работающей по принципу «одного окна». Стратегия государственной трансформации Великобритании, опубликованная в 2017 г., устанавливает курс на дальнейшее развитие электронного правительства, воспитание людей, развитие культуры и компетенций, разработку усовершенствованных инструментов, технологий и методов государственного управления, оптимизацию использования данных и создание единых платформ, компонентов и мощностей для бизнеса.

В Туркменистане работы по созданию электронного правительства фактически только начинаются. В конце ноября 2018 г. Президент Туркменистана утвердил своим указом «Концепцию развития цифровой экономики на 2019-2025 годы», которая направлена на повышение эффективности работы всех отраслей экономики и общественной сферы страны за счёт использования информационных технологий. Концепция включает 7 глав, отражающих современное состояние системы информационно-коммуникационных технологий Туркменистана, цели, задачи, пути и механизмы их развития, а также ожидаемые результаты. Выполнение задач, описанных в документе, разделено на 3 этапа: первый – 2019 год, второй – 2020-2023 годы и третий – 2024-2025 годы. Подписав постановление об утверждении документа, туркменский лидер выразил уверенность, что последовательное выполнение его положений окажет содействие дальнейшему прогрессу страны, деловой и инвестиционной активности, внедрению передовых методов государственного управления, созданию новых рабочих мест.

В странах первой десятки процесс построения электронного правительства находится на пятом этапе, в Российской Федерации, Республике Беларусь и Казахстане – на четвертом этапе, а в Туркменистане – на первом этапе. Результаты проведенного анализа мирового опыта внедрения информационных технологий в государственное управление будут положены в основу предложений по дальнейшему развитию применения информационных технологий в государственном управлении Туркменистана.

Список использованных источников:

1. Ямщиков, А.С. Национальные системы электронного правительства / А.С. Ямщиков, Д.А. Баранов // Научное обозрение. Экономические науки. – 2017. – № 2. – С. 145-151.

2. Исследование ООН: Электронное правительство 2018 – [Электронный ресурс]. – Режим доступа: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_Russian.pdf – Дата доступа: 28.02.2019.

3. Agency for Digitisation Denmark (2016). A Stronger and More Secure Digital Denmark (2016-2020). – [Электронный ресурс]. – Режим доступа: https://digst.dk/media/16165/ds_singlepage_uk_web.pdf. – Дата доступа: 28.01.2019.

МЕТОДЫ МОНИТОРИНГА КЛАСТЕРНЫХ СЕРВИСОВ В ОБЛАСТИ ЭЛЕКТРОННОЙ КОМЕРЦИИ

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

Жук П.Б., Бобов М.Н.

В этой работе рассмотрены основные метрики и методы, применяемые для мониторинга кластерных сервисов в области электронной коммерции.

В настоящее время для обеспечения высокой доступности веб-сервисов, масштабирования, балансирования трафика, данных между несколькими серверами широко используется подход размещения одного сервиса в кластере серверов.

При таком подходе понимание состояния инфраструктуры и систем важно для стабильной работы сервисов. Информация о работоспособности и производительности развертываний не только помогает вовремя реагировать на проблемы, но и дает возможность уверенно вносить все требуемые изменения. Один из способов получить эту информацию – это система мониторинга, позволяющая осуществлять сбор метрик, визуализацию данных и нотификацию в случае неправильной работы кластерных сервисов.

Мониторинг – это процесс сбора, агрегирования и анализа этих данных для улучшения понимания характеристик и поведения компонентов системы. Данные из разных точек среды собираются системой мониторинга, которая отвечает за хранение, агрегацию, визуализацию данных и автоматические реагирует на изменения, когда значения соответствует заданным условиям.

Метрики, мониторинг и система оповещений составляют основу системы мониторинга и позволяют отразить состояние системы, отследить тенденции в потреблении ресурсов или поведении, а также влияние вносимых изменений.

Одной из функций систем мониторинга является организация и корреляция данных из различных источников. Эффективность показателей мониторинга можно оценить возможностью администратора шаблоны поведения между разными ресурсами и группами серверов.

В основном, выделяют четыре вида метрики для осуществления мониторинга: задержка ответа сервиса, уровень входящего трафика, ошибки, занятость ресурсов.

Задержка – это время, необходимое для завершения действия. Специфика измерения этой метрики зависит от компонента, ее общие аналоги – время обработки, время отклика.

Задержка показывает, как долго будет выполняться конкретная задача или действие. Измерение задержки различных компонентов позволяет построить целостную модель различных характеристик системы. Это может помочь найти узкие места и определить каким ресурсам нужно больше всего времени, и своевременно обратить внимание на замедление работы системы. Следует подчеркнуть, что при расчете задержек важно учитывать как успешные, так и неуспешные запросы, поскольку они могут искажать средние значения сервиса.

Уровень трафика обозначает занятость ресурсов системы. Это нагрузка на сервисы, которая позволяет определить количество входящего и исходящего трафика, обрабатываемого системой в настоящее время.

Ошибки и их количество позволяют иметь более полную картину состояния компонентов и их реакции на запросы. Разделяя различные типы ошибок, возможно более точно определить проблемы, влияющие на приложения. Это также позволяет настроить гибкую систему оповещений: об отдельных типах ошибок система может оповещать немедленно, а другие игнорировать, пока они не превышают определенный порог.

Данные **использования ресурсов** предоставляют информацию о ресурсах, от которых зависит эффективность сервиса. Поскольку работа сервиса, который предоставлен одним компонентом, может требоваться для работы другого сервиса, использование ресурсов является одним из важнейших показателей для определения проблем с пропускной способностью. Проблемы использования ресурсов и задержки в одном слое могут отображать существенный скачок трафика или наличие ошибок в нижнем слое.

На основании вышеперечисленных метрик существует 2 метода мониторинга кластерных сервисов: USE и RED.

USE (utilization, saturation, errors) метод предназначен для выявления проблем в производительности ресурсов и основан на измерении трех основных метрик использование ресурсов:

1. Использование (англ. utilization) – время, в течение которого ресурс был занят обработкой полезного трафика.
2. Насыщение (англ. saturation) – степень загруженности ресурса, т.е. отношение необработанного трафика к обработанному.

3. Ошибки (англ. errors) – количество ошибок при обработке.

RED (rate, errors, duration) метод сосредоточен на выявлении ошибок, не связанных в большинстве с производительности (ошибки логики программы, неправильной конфигурации) и основан на трех метриках.

1. Темп (англ. rate) – количество успешно обработанных запросов за единицу времени.
2. Ошибки (англ. errors) – количество неудачно обработанных запросов за единицу времени.
3. Длительность (англ. duration) – интервал времени, необходимый для обработки запроса.

Оба метода обеспечивают оценку работы кластерных сервисов, однако только совместное использование данных методов может обеспечить более высокий уровень качества мониторинга сервисов.

Список использованных источников:

1. Newman, S. Building Microservices // O'Reilly Media, Inc. – 2016 – Piter Press Ltd.– P. 197 – 205
2. Beyer, B. Site Reliability Engineering. / C. Jones, J. Petoff, N. R. Murphy // O'Reilly Media, Inc. – 2016 – P. 50 – 67

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ СЕТЕВЫХ КОМПОНЕНТОВ СИСТЕМЫ «УМНОГО ДОМА»

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

Алисеенко М.А., Никульшин Б.В.

Никульшин Б.В. – к.т.н., доцент

Рассмотрены структура и функционирование системы "умного дома". Описаны ее функциональные компоненты устройств. Разработан подход тестирования сетевых компонентов «умного дома» для оценки их функционирования и взаимодействия.

В настоящее время актуальной задачей является формирование стратегии тестирования компонентов «умного дома», обеспечивающей качество предоставляемых пользователю услуг [1-2]. В системе взаимодействие устройств осуществляется по сети, состояние которой может повлиять на производительность, качество работы устройств и инфраструктуры в целом [3]. Для проверки работоспособности компонентов необходимо выделить функциональные блоки у устройств, отвечающие за одни и те же управляющие команды. Предложенный подход к тестированию сетевых компонентов системы «умного дома» обеспечивает уменьшение временных затрат на проведение проверки всех компонентов.

Функциональное тестирование сетевых компонентов «умного дома» предлагается разделить на уровни: проверка физических параметров, проверка программного обеспечения устройств, проверка взаимодействия низко- и высокоуровневых компонентов.

На первом уровне пульты (PR) и датчики (PT) проверяются на выделение несущей частоты. Блоки питания и силовые элементы подвергаются имитации частого включения и выключения из сети, что может привести к выходу из строя внутренних компонентов. Управляющие элементы проверяются на соответствие максимальной выходной характеристике мощности. Все типы устройств должны принимать и отправлять команды на расстоянии, соответствующем техническим характеристикам.

На втором уровне функциональные компоненты тестируются на корректность отработки запрограммированных команд. Базовый набор команд для силовых блоков включения (on, switch), выключения (off), привязки (bind), отвязки (unbind) возможно проверить с помощью универсального пульта. В каждый силовой блок вшит идентификатор универсального пульта, благодаря чему он не требует стандартной привязки пользовательского пульта или датчика. Стандартная привязка, отвязка и очистка памяти должна подтвердится на силовом блоке нажатиями сервисной кнопки, что занимает больше временных ресурсов, рис.1. Шесть операций проверки можно свести к трем.

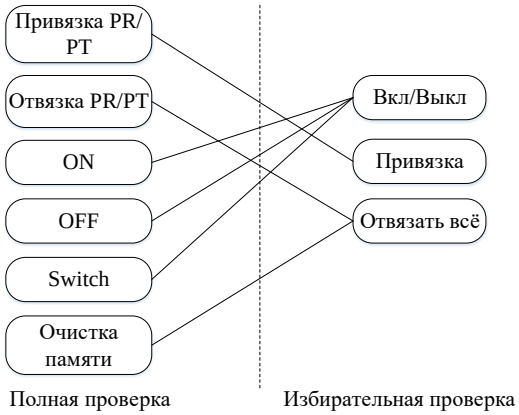


Рисунок 1 – Проверка силовых блоков с помощью универсального пульта

Третий уровень включает проверку управления устройствами посредством пользовательского программного обеспечения, которое обеспечивает Ethernet-шлюз. Команды, поддерживаемые устройствами можно разделить на подгруппы и посылать группами на тестовый стенд, вместо поочередной отправки.

Список использованных источников:

1. Борисова М. В., Киричек Р. В. Методы тестирования технологий передачи данных устройств Интернета Вещей // Информационные технологии и телекоммуникации. 2018. Том 6. № 2. С. 27–34.

2. Киричек Р. В. Методы исследования беспроводных каналов связи Интернета вещей в условиях совместной работы / В. А. Кулик, Р.В. Киричек, А. Н. Бондарев // Информационные технологии и телекоммуникации. 2015. № 2 (10) С. 106-114.

3. Долгушев Р. А., Киричек Р. В., Кучерявый А. Е. Обзор возможных видов и методов тестирования Интернет Вещей // Информационные технологии и телекоммуникации. 2016. Том 4. № 2. С. 1–11.

СРАВНИТЕЛЬНАЯ ОЦЕНКА ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ ПРИ ИСПОЛЬЗОВАНИИ РАЗНЫХ ТИПОВ КОДОВ

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

Серченя А.А.

Липкович Э.Б. – доцент

Применение помехоустойчивого кодирования с исправлением ошибок в современных системах связи является обязательным. Кодирование информации позволяет, с одной стороны, уменьшить количество ошибок в канале, возникающих из-за влияния частотно-селективных замираний, индустриальных помех и прочих факторов, и тем самым уменьшить общее время неготовности линии связи, и с другой стороны, снизить значение пороговой чувствительности приемника, за счет чего можно увеличить энергетику линии связи.

За последние годы в технику связи успешно внедрены многопороговые декодеры, декодеры максимального правдоподобия Витерби, коды Рида-Соломона (РС), каскадные схемы кодирования, алгоритмы турбокодов и др. Однако требования к алгоритмам коррекции ошибок в каналах связи с помехами непрерывно растут. При этом сохраняется основная проблема – декодирование с эффективностью, близкой к оптимальной, при существующем ОСШ в канале связи.

На сегодняшний день известно много различных классов помехоустойчивых кодов, отличающихся друг от друга структурой, функциональным назначением, энергетической эффективностью, алгоритмами кодирования и декодирования и многими другими параметрами. Среди всего разнообразия классификации выделим два вида кодов: блочные и непрерывные. К первым относится код Рида-Соломона, недвоичный циклический блоковый код, отличающиеся наличием минимального кодового расстояния Хэмминга $d_м$ среди блочных кодов с равной величиной $R_к$. Среди непрерывных кодов можно выделить сверточные, наиболее распространенные в системах связи благодаря тому, что в каналах с белым гауссовским шумом (БГШ) их использование позволяет получить весьма существенный энергетический выигрыш от кодирования (ЭВК) при относительно простой реализации декодера. Рассмотрим эти два вида кодов и сравним их энергетическую эффективность.

Требуемое отношение сигнал/шум и энергетический выигрыш от кодирования можно вычислить несколькими способами. Первый – это классический способ, трудоемкий и времязатратный, предполагающий знание весовых коэффициентов для каждого вида модуляции и использование сложной вычислительной техники. Однако в данной статье для вычисления требуемых характеристик используется другой способ – математические модели, значительно упрощающие расчеты, использующие при этом лишь основные параметры модуляции и кодирования (свободное расстояние сверточного кода $d_с$, минимальное кодовое расстояние Хэмминга $d_м$, порядок модуляции m, относительная скорость кода $R_к$.

В таблице 1 представлены формульные соотношения для определения требуемого отношения сигнал/шум и энергетического выигрыша от кодирования при использовании сверточного кодирования и кодирования кодами Рида-Соломона. Как можно заметить, формульные соотношения имеют сходную структуру для обоих видов кодов. Подобные им математические модели были разработаны также и для других видов кодов (кодов Хэмминга, БЧХ-кодов и др.) и являются гораздо более простыми и эффективными в использовании. Параметры C_i, q_i, использованные в формулах, представляют собой коэффициенты, зависящие от вида модуляции.

Таблица 1 - Формульные соотношения расчета энергетического выигрыша от кодирования для СК и кодов РС

СК	Коды РС
1	2
$h_к = 10\lg\left[\frac{2,3\cdot(D_м - 0,5\cdot\lg(2.3D_м/\mu_м))}{\mu_м}\right]$, дБ	$h_к = 10\lg\left[\frac{2,3\cdot(B - 0,5\cdot\lg(2.3B/\mu))}{\mu}\right]$, дБ
$\Delta G_к = h_0 - h_{0к} = 10\lg R_к \cdot d_с \cdot \beta \cdot \xi$, дБ	$\Delta G_к = h_0 - h_{0к} = 10\lg R_к \cdot (t+1) \cdot \beta \cdot \xi$, дБ
$\xi = \frac{A - 0,5\lg(2,3A/q_i)}{D_м - 0,5\lg(2,3D_м/\mu_м)}$	$\xi = \frac{A - 0,5\lg(2,3A/q_i)}{B - 0,5\lg(2,3B/\mu)}$
$\mu_м = R_к d_c \beta_м q_i$	$\mu = R_к (t+1) \beta q_i$
$\beta_м = [1 - L_м/(6\sqrt{P_b}(1-R_к)\cdot L_м - \lg P_b)]/Q$, дБ	$\beta_м = [1 - L_д/(3,5\sqrt{P_b}\cdot L_д - \lg P_b)]/Q$, дБ
$L_м = \lg(R_к d_c \sqrt{d_c q_i})$	$L_д = \lg(R_к (t+1)\sqrt{d_м q_i})$

1	2
$A = -\lg P_b - \lg \frac{\sqrt{\pi q_i}}{C_i}$	$A = -\lg P_b - \lg \frac{\sqrt{\pi q_i}}{C_i}$
$D_м = -\lg P_b - \lg \frac{\sqrt{\pi q_i}}{C_i} \cdot (2N-3) + \lg(\sqrt{\frac{\mu}{q_i}})$, дБ	$B = -\lg P_b - \lg \frac{\sqrt{\pi q_i}}{C_i} + \lg(\sqrt{\frac{\mu}{q_i}})$, дБ
$Q = 1 + \frac{0,8\sqrt{P_b}}{(1-R_к)}$	$Q = 1 + \lg \frac{(t+1)n}{2t(-\lg P_b)}$

Кривые помехоустойчивости, полученные вышеобозначенным способом, идентичны тем, что рассчитываются при использовании классического метода их получения с помощью весовых коэффициентов. При расчете получаем, что в области значения ошибок от 10-2 до 10-10 кодирование с помощью РС кода проигрывает сверточному коду с $R_{ск}$ = 0,75 по величине ОСШ (около 1 дБ для P_b = 10^{-5}) всех рассматриваемых порядков КАМ модуляции и в области значений от 10^{-3} до 10^{-8} РС коды проигрывают сверточному коду при использовании ФМ-М видов модуляции. Соответственно, использование того или иного кода обусловлено величиной вероятности ошибки.

Рассмотрим сравнение кодов еще по одной крайне важной энергетической характеристике – энергетическому выигрышу от кодирования (ЭВК). На рисунке 1 представлены зависимости энергетического выигрыша от кодирования при использовании квадратурно-амплитудной модуляции разного порядка.

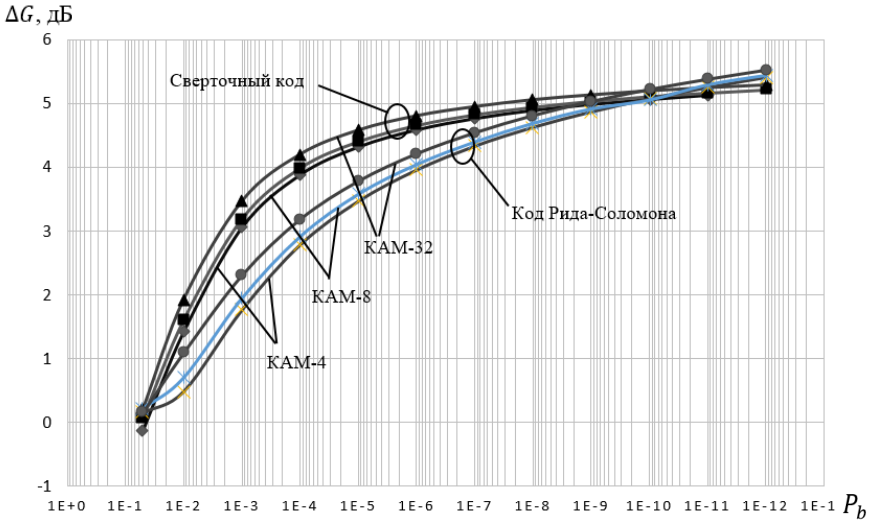


Рисунок 1 – Зависимости $\Delta G = f(P_b)$ для КАМ-М модуляции при использовании РС и сверточных кодов

Анализ приведенных зависимостей показывает, что в зоне ошибок от 10^{-2} до 10^{-8} сверточное кодирование обладает преимуществами в ЭВК и, следовательно, в энергетической эффективности перед кодом РС с принятыми параметрами. Аналогичное поведение ЭВК для сравниваемых кодов характерно и для каналов с многопозиционной фазовой модуляцией. Различие в ЭВК между зависимостями для P_b = 10^{-5} составляет около 1 дБ.

Имеется еще рад характеристик, которые характеризуют тот или иной помехоустойчивый код, однако, как видно из статьи, по энергетическим характеристикам сверточный код обладает преимуществом по отношению в коду Рида-Соломона, что весьма важно для современных систем радиорелейной связи, т.к. это позволяет иметь меньшее ОСШ на входе приемного устройства.

Список использованных источников:

1. Липкович, Э. Б. Цифровые системы радиосвязи и радиовещания : электронный ресурс по учебной дисциплине / Э. Б. Липкович [Электронный ресурс]. – Минск : БГУИР, 2016. – Режим доступа: http://www.bsuir.by/

2. Золотарёв, В.В., Овечкин, Г.В. Помехоустойчивое кодирование. Методы и алгоритмы : Справочник / Ю.Б. Зубарев, – М.: Горячая линия-Телеком, 2004. – 126 с.

SDM-WDM-PON

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

Сергеев Н.Н.

Урядов В.Н. – к.т.н.,доцент

С появлением множества широкополосных интернет-сервисов, таких как облачные вычисления, телевидение высокой четкости (HD) / 4K, бизнес-IP-трафик и социальные сети, в сетях доступа наблюдается экспоненциальный рост спроса на пропускную способность.

Для увеличения пропускной способности системы PON было введено мультиплексирование с пространственным разделением (SDM), чтобы использовать несколько пространственных каналов для передачи данных через одно волокно [1]. В сети SDM-WDM-PON, используется модуляция интенсивности и прямое обнаружение (IM / DD) с многоядерным волокном и низким уровнем перекрестных помех (MCF) без какой-либо цифровой обработки сигналов (DSP). 7-ядерное волокно используется для демонстрации концепции, где три внешних ядра используются для восходящего потока а три других внешних ядра используются для нисходящего потока (DS). Внутреннее ядро в центре используется для передачи источника света, исходящего от оптического линейного терминала (OLT), к ONU.

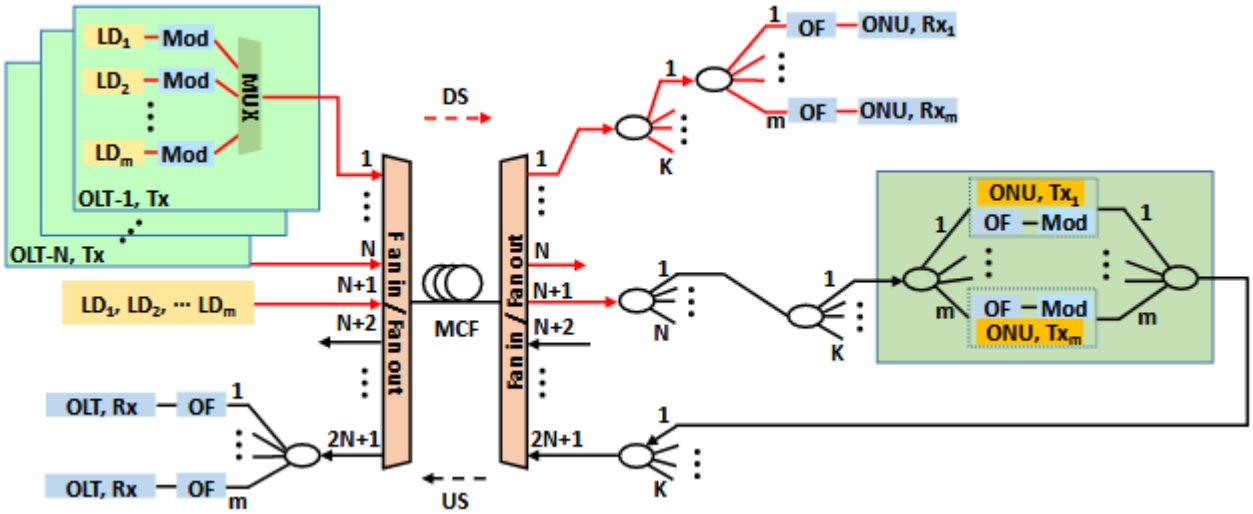


Рисунок 1 – Предлагаемая архитектура SDM-WDM-PON

Предложенная архитектура SDM-WDM-PON показана на рисунке 1. В каждом подмножестве OLT имеется m передатчиков на разных длинах волн (от λ1 до λm), которые отправляют сигналы на одно из ядер MCF. Всего имеется N OLT (от OLT-1 до OLT-N), которые представляют количество ядер для передачи DS и могут совместно использовать лазерные источники. Требуются только m лазеров, и каждый выход лазера делится на N раз для каждого OLT. Благодаря совместному использованию лазерного источника стоимость на стороне OLT будет снижена. Сигналы от OLT мультиплексируются по длине волны с помощью мультиплексоров WDM (MUX), а затем поступают в MCF через устройство разветвления. После передачи MCF сигналы сначала демультиплексируются SDM в N-одномодовых волокон (SMF) с помощью устройства разветвления, и сигналы в каждой SMF делятся на коэффициент K и отправляются в ONU. В каждом ONU есть N SMF для канала DS, которые можно упаковать в виде волоконной ленты для простоты управления. В каждой SMF имеется m сигналов на длинах волн от λ1 до λm, которые WDM демультиплексируются с помощью ответвителя и фильтров, а затем обнаруживаются фотодетекторами[2]. Совокупная пропускная способность в SDM-WDM-PON достигает 300 Гбит/с., такая сеть может быть хорошим вариантом для будущих сетей широкополосного доступа, транспортных сетей, сетей 5G.

Список использованных источников:

1. H. Hu, R. Asif, F. Ye, S. Gross, M. Withford, T. Morioka, and L. K. Oxenlowe, “Bidirectional 120 Gbps SDM-WDM-PON with Colourless ONU using 10 Gbps Optical Components without DSP,” in Optical Fiber Communication Conference - America, 2016 – 15 S.

2. F. Ren, J. Li, Z. Wu, T. Hu, J. Yu, Q. Mo, Y. He, Z. Chen, and Z. Li, “Three-mode mode-division-multiplexing passive optical network over 12-km low mode-crosstalk FMF using all-fiber mode MUX/DEMUX,” Opt. Commun. 383, 525–530 (2017).Rüthers, B. Rechtstheorie: Begriff, Geltung und Anwendung des Rechts / B. Rüthers, Ch. Fischer. – 5. Aufl. – München : Beck, 2010. – 665 S.

РОЛЕВОЙ ДОСТУП В СИСТЕМАХ ЗИ

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

Климов Д.А., Ширинский В.П., Некрашевич И.Г.

Ширинский В.П. – к.т.н.,доцент

В работе приводится описание построения ролевого управления доступом в системах ЗИ. Формулируются определения базовых элементов и механизмов ролевой модели.

При большом количестве пользователей традиционные системы управления доступом становятся сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимо решение эту сложность понизить.

Таким решением является ролевое управление доступом. Суть его в том, что между пользователем и его привилегиями появляется промежуточная сущность – роль. Для каждого пользователя могут быть активными несколько ролей, каждая из которых дает ему определенные права.

Ролевой доступ облегчает администрирование, так как делает систему разграничения доступа управляемой при большом числе пользователей. Ролей может быть значительно меньше, чем пользователей.

Ролевое управление доступом оперирует следующими понятиями:

- пользователь;
- сеанс работы;
- роль;
- объект;
- операция.

Ролям приписываются пользователи и права доступа. Вводится понятие разделения обязанностей в двух видах: статическом и динамическом.

Статическое распределение обязанностей налагает ограничение на приписывание пользователей ролям. Членство в некоторой роли запрещает приписывание пользователя определенному множеству других ролей.

Динамическое распределение обязанностей отличается от статического тем, что рассматриваются роли, одновременно активные (в разных сеансах) для данного пользователя (а не те, к которым пользователь статически приписан).

Рассматриваются 3 категории функций:

- административные (создание и сопровождение ролей и других атрибутов ролевого доступа);
- вспомогательные (обслуживание сеансов работы пользователей);
- информационные (получение сведений о текущей конфигурации).

Список использованных источников:

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.: ил. — (Профессиональное образование)

2. Сердюк В.А. Новое в защите от взлома корпоративных систем Москва: Техносфера, 2007. - 360с.

3. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. – М.: Книжный мир, 2009

4. Галатенко В.А. Основы информационной безопасности: учебное пособие : для студентов вузов по спец. 351400 "Прикладная информатика" / Галатенко В.А., под ред. Бетелина В.Б. - 4-е изд. - Москва: Интернет-Университет Информационных Технологий, Москва: БИНОМ. Лаборатория знаний, 2012. - 205 с.: ил., табл.

МОДУЛЬ ВЗАИМОДЕЙСТВИЯ В РЕАЛЬНОМ ВРЕМЕНИ В СИСТЕМЕ УПРАВЛЕНИЯ МЕРОПРИЯТИЯМИ

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

Шабловский И.И.

Чепикова В.В. – ассистент

В наши дни скорость и стабильность интернет-соединения достигли больших высот, что открывает большое количество возможностей для разработчиков и пользователей. Так, становится доступной такая опция, как взаимодействие в реальном времени. Многие современные приложения используют взаимодействие в реальном времени, что улучшает пользовательский опыт, путем упрощения и ускорения взаимодействия пользователя с системой.

В последние 10 лет множество приложений начало и успешно использует взаимодействие в реальном времени. Было разработано множество технологий для обеспечения взаимодействия между веб-приложением и сервером, например, Long polling, Forever Frames, Server-Sent Events, WebSockets. Наиболее современным решением из является использование протокола WebSocket.

Реализацию и эксплуатацию системы взаимодействия в реальном времени рассмотрим на примере системы управления мероприятиями. Данная система позволяет пользователям создавать, отслеживать, искать мероприятия, находить участников, волонтеров и многое другое.
В рамках данной системы, модуль взаимодействия в реальном времени используется для уведомления пользователя об изменениях в интересующих его мероприятиях, новых приглашениях и сообщениях.

Для реализации модуля уведомлений в реальном времени была выбрана библиотека SignalR, с использованием сервиса Azure SignalR, для улучшения масштабируемости системы. Библиотека позволяет использовать все вышеперечисленные механизмы для передачи запросов между клиентом и сервером в реальном времени. Библиотека предлагает реализацию взаимодействия по схеме “Хаб-Клиент”, хаб представляет собой набор соединений, а также предоставляет им некоторый интерфейс для взаимодействия.

Для каждого типа уведомлений был разработан хаб с соответствующим интерфейсом взаимодействия.

При всех своих преимуществах, системы взаимодействия в реальном времени имеют ряд недостатков, главным из которых являются относительно высокие требования к скорости и стабильности интернет-соединения. Второе решается с помощью механизмов переподключения, а чтобы не занимать всю ширину канала, следует провести оптимизацию запросов - уменьшить их количество и объем передаваемых данных. Рассмотрим несколько эффективных способов оптимизации запросов: использование GraphQL, zip-сжатие HTTP запросов-ответов, использование JSON как формата передаваемых данных.

- GraphQL - язык запросов, а также исполняющая среда для создания REST API. Важнейшей особенностью является конфигурирование запроса на получение данных на клиенте. Это значит, что системе не придется передавать информацию, которая не используется, а также позволит сократить количество запросов, путем получения всех необходимых данных за один запрос.

- Также для уменьшения объема передаваемых данных можно использовать JSON - формат организации данных. По сравнению с классическим форматом XML его проще читать и, при одинаковых данных, объем служебной информации в JSON файле значительно меньше.

- Также протокол HTTP поддерживает возможность сжатия данных без потерь по алгоритму ZIP, что также уменьшает объем передаваемой информации.

Список использованных источников:
1. Facebook OpenSource https://graphql.org
2. Microsoft https://docs.microsoft.com/en-us/aspnet/signalr/overview/

СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ АВТОСАЛОНА VOLVO

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

Каплич А.А.

Чепикова В.В.. – ассистент, магистр технических наук

Окружающий нас мир и современный ритм жизни, угрозы террористов и криминальных элементов заставляют многие учреждения, организации, а также обычных людей осуществлять контроль окружающей обстановки. Поэтому все более популярными в нашей жизни становятся системы видеонаблюдения.

Их функция заключается не только в передаче изображения на монитор, но и в выделении некоторых важных элементов, например, распознавание лица человека или номера автомобиля. В этом случае системы видеонаблюдения – подобие зрения человека. Происходит взаимодействие с участием воспринимающего и анализирующего устройств.

Разновидности видеонаблюдения:

1. Аналоговые
2. Цифровые

Главным отличием цифровой технологии в видеонаблюдении от аналоговой, является повышенное качество картинки на экране. Естественно, что стоимость таких систем намного выше. Рассмотрим подробнее их устройство.

В настоящее время существует большое количество аналоговых и цифровых видеокамер:

1. Купольные
2. Цилиндрические
3. Микрокамеры
4. Уличные
5. Инфракрасные

Аналоговое видеонаблюдение.

На рисунке 1 представлена простейшая схема аналогового видеонаблюдения.

Рис.1 – Схема аналогового видеонаблюдения.

Достоинства:

1. Простая установка и настройка.
2. Хорошая совместимость разных типов камер.
3. Низкая стоимость комплектующих.

Недостатки:

1. Затруднительное масштабирование крупных систем.
2. Невозможно зашифровать видеосигнал.
3. Нет защиты от помех.
4. Нет таких полезных функций: детектор движения, встроенное аудио, цифровое увеличение, наклон и поворот камеры по одному кабелю.

Цифровые системы видеонаблюдения

На рисунке 2 представлена схема цифрового видеонаблюдения.

Рис.2 – Схема цифрового видеонаблюдения.

Цифровое видеонаблюдение делится на компьютерные системы и отдельное оборудование. Цифровая запись видео осуществляется устройствами, функционирующими на компьютере, с приложением плат видео захвата. Компьютерный вид видеонаблюдения имеет значительно больше функций, по сравнению с некомпьютерным. На базе компьютера видеонаблюдение можно легко модернизировать, настроить широкие возможности управления. Особенностью некомпьютерных устройств видеонаблюдения является отсутствие аудио входов.

Достоинства:

1. Возможность создать видеонаблюдение на основе локальной сети учреждения.
2. Возможность оперативного переноса видеонаблюдения на другие компьютеры.
3. Простое совмещение системы видеонаблюдения с разными системами безопасности, а также ее модернизация.
4. Видеосигнал защищен от несанкционированного доступа.
5. Повышенное качество изображения на мониторе, полученное от цифровой камеры.

Недостатки:

1. Непростая настройка камер.
2. Требуется большой объем памяти для хранения видео файлов, ввиду их высокого качества.

Видеорегистраторы и платы видео захвата.

Существует много различных устройств для видео захвата изображения. Наиболее популярными стали видеорегистраторы и платы видео захвата.

Видеорегистраторы производят в виде самостоятельного устройства. Они имеют такие же параметры, как и платы видео захвата, однако число функций у них намного больше. Это устройство может передавать информацию на компьютер, оснащено внутренней памятью для хранения файлов видео, может работать с сетевыми протоколами передачи информации на удаленный компьютер. Такой тип оборудования видео захвата применяется при необходимости подключения большого числа камер, а также при необходимости соединения с удаленным компьютером для хранения информации, например, в большом супермаркете.

Платы видео захвата являются наиболее простыми устройствами, которые не могут функционировать отдельно от компьютера, и без специальной программы. Они могут использоваться только в системе с малым количеством камер. В бытовых условиях плата видео захвата является оптимальным вариантом для использования в видеонаблюдении. Запись видео файла производится непосредственно на винчестер компьютера. Поэтому, необходимо заранее обеспечить наличие свободного объема памяти на диске. При подборе платы видео захвата обращают внимание на число камер и на формат файла видео, а также на скорость захвата и на разрешение видео изображения.

Список использованных источников:

1. Герман Кругль (Herman Kruegle). "Профессиональное видеонаблюдение. Практика и технологии аналогового и цифрового CCTV". "Секьюрити Фокус" (Security Focus), 2010.
2. Андрей Кашкаров. Системы видеонаблюдения. 2014г.

ПРЕДВАРИТЕЛЬНАЯ ОБРАБОТКА АСМ-ИЗОБРАЖЕНИЙ

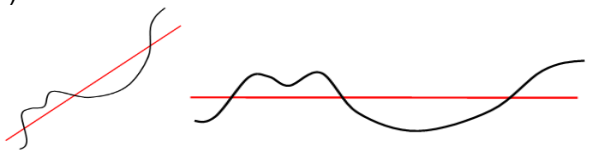
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

М.В. Козак

Рассмотрены методы предварительной обработки изображений с атомно-силового микроскопа.

При обработке изображений используются различные методы, для улучшения последующего анализа изображений: вычитание среднего наклона, усреднение и медианная фильтрация, подсветка объекта.

Изображения, полученные с помощью атомно-силового микроскопа могут иметь наклон поверхности образца либо смещение образца во время сканирования при температурном дрейфе. Такие наклоны могут влиять на определение структуры объекта. Чтобы исключить это необходимо из исходной матрицы значений вычесть плоскость среднего наклона Вычитание среднего наклона представлено на рисунке 1(а, б).



а *б*

Рис. 1 – Вычитание среднего наклона: *а* – исходный профиль поверхности; *б* – поверхность после вычитания среднего наклона

В результате получаем матрицу с меньшим диапазоном значений, следовательно, мелкие детали становятся более заметными.

Изображение помимо полезного сигнала имеет шумовую составляющую. Чтобы убрать шум необходимо заменить значение точки изображения средним арифметическим значением всех точек ближайшей окрестности. При высоком уровне шумов необходимо расширить размер окрестности, по которой делается усреднение.

Если требуемый результат нельзя достичь усреднением по окрестности, применяется медианная фильтрация. При таком методе значение в точке фильтрации заменяется на среднее значение соседних точек. Медианная фильтрация позволяет убрать резкие перепады, но при этом не так сильно сглаживает изображение, как метод усреднения по окрестности.

Для того, чтобы лучше различать мелкие детали на поверхности, необходимо увеличить контрастность объекта и основного фона. На изображении необходимо создать эффект освещения (рисунок 2), тогда мелкие детали станут различимы, без потери информации о более крупных объектах. Но при таком методе значительно искажается информация о высоте объекта

а *б* *в*

Рис. 2 – Изображение для обработки: *а* – исходное изображение; *б*, *в* – изображение, с применение подсветки различной интенсивности

Для анализа изображений с атомно-силового микроскопа необходима предварительная обработка. В зависимости от задач, необходимо ли рассмотреть мелкие детали, либо нужно все изображение целиком, применяются различные методы обработки: вычитание среднего наклона, усреднение по окрестности, медианная фильтрация, подсветка и другие.

Список использованных источников:

1. Image processing; analysis and machine vision / Milan S. [et al.]. Thomson press, west, 2008. – P. 175-240.
2. Gonzales, R.C. Digital image processing / R.C. Gonzales, R.E. Woods. – Pren-tice-Hall, 2002. – 793 p.

АКТУАЛЬНОСТЬ СТАНДАРТА WI-FI 802.11N

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

Криводубский А.В., Краснов А.И.

Рабцевич В.В. – ассистент

Wireless LAN или, как часто употребляется в странах СНГ, БЛВС (Беспроводная Локально-Вычислительная Сеть) стандарта Wi-Fi 802.11 разрабатывалась для решения задачи беспроводного широкополосного доступа к сетям передачи данных на высоких скоростях. Основная цель и смысл технологии это предоставление мобильности пользователям с разными типами носимых устройств:лаптопы/нетбуки, планшетные компьютеры, смартфоны, Wi-Fi радиотелефоны (VoIP over Wi-Fi) и т.п.

Пользователь доступа стандарта Wi-Fi становится не привязанным к конкретному столу или розетке Ethernet, а может перемещаться по всему офису или всей зоне покрытия сети Wi-Fi и везде иметь доступ к данным безопасно, надежно и быстро.

IEEE 802.11n – самый передовой коммерческий Wi-Fi - стандарт, на данный момент, официально разрешенный к ввозу и применению на территории РБ. Совместим с 11b/11a/11g. Хотя рекомендуется строить сети с ориентацией только на 802.11n, т.к. требуется конфигурирование специальных защитных режимов при необходимости обратной совместимости с устаревшими стандартами. Это ведет к большому приросту сигнальной информации и существенному снижению доступной полезной производительности радиоинтерфейса. Стандарт ***IEEE 802.11n*** основан на технологии OFDM-MIMO (Multiple Input Multiple Output). Очень многие реализованные в нем технические детали позаимствованы из стандарта 802.11a, однако в стандарте IEEE 802.11n предусматривается использование как частотного диапазона, принятого для стандарта IEEE 802.11a, так и частотного диапазона, принятого для стандартов IEEE 802.11b/g. То есть устройства, поддерживающие стандарт IEEE 802.11n, могут работать в частотном диапазоне либо 5, либо 2,4 ГГц, причем конкретная реализация зависит от страны. Увеличение скорости передачи в стандарте IEEE 802.11n достигается, во-первых, благодаря удвоению ширины канала с 20 до 40 МГц, а во-вторых, за счет реализации технологии MIMO.

Технология MIMO (Multiple Input Multiple Output) предполагает применение нескольких передающих и принимающих антенн. По аналогии традиционные системы, то есть системы с одной передающей и одной принимающей антенной, называются SISO (Single Input Single Output).

Теоретически, MIMO-система с *n* передающими и *n* принимающими антеннами способна обеспечить пиковую пропускную способность в *n* раз большую, чем системы SISO. Это достигается за счет того, что передатчик разбивает поток данных на независимые последовательности бит и пересылает их одновременно, используя массив антенн. Такая техника передачи называется **пространственным мультиплексированием.** Отметим, что все антенны передают данные независимо друг от друга в одном и том же частотном диапазоне.

В стандарте IEEE 802.11n предусмотрены как стандартные каналы связи шириной 20 МГц, так и каналы с удвоенной шириной. Однако применение 40-мегагерцевых каналов является опциональной возможностью стандарта, поскольку использование таких каналов может противоречить законодательству некоторых стран.

Таблица 1 – Характеристики стандарта IEEE 802.11n

Скорость передачи данных, Мбит/с	Обязательная поддержка скорости, Мбит/с	Число каналов	Расстояние и скорость передачи данных	Используемые ключевые технологии	Рабочая частота
До 54	Основные: 6; 12; 24	52 (56) при ширине 20 МГц; 104 (114) при ширине 40 МГц	В закрытых помещениях: 12 м (54 Мбит/с); 91 м (6 Мбит/с)	Мультиплексирование с разделением по ортогональным частотам (OFDM) (с использованием технологии MIMO)	2,4 ГГц (2,4-2,4835 ГГц) 5 ГГц (5,15-5,350 ГГц и 5,725-5,825 ГГц)
	Дополнительные: 9; 18; 36; 48; 54		В открытых помещениях в пределах прямой видимости: 30 м (54 Мбит/с); 305 м (6 Мбит/с)		

Список использованных источников:

1. Wi-Life: Wi-Fi стандарты. [Электронный ресурс]. – Режим доступа: www.wi-life.ru. – Дата доступа: 28.03.2019.

2. Компьютерная компания НИКС: Общие сведения о Wi-Fi. [Электронный ресурс]. – Режим доступа: www.nix.ru. Дата доступа: 28.03.2019.

3. Компьютерные сети: учеб. пособие для студентов высших учебных заведений по техническим специальностям/ П.П. Урбанович, Д.М. Романенко, Е.В. Кабак. – Минск: БГТУ, 2011. – 400 с.

ЗАЩИТА МНОГОВОЛНОВЫХ ВОСП ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

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

Дудак М.Н.

Урядов В.Н. – к.т.н., доцент

Связь с использованием оптоволокна далеко не так защищена, как это обычно принято считать. Существует ряд известных методов, используемых для извлечения или вставки информации в оптический канал и позволяющих избежать обнаружения подключения. В данной работе рассматривается способ снятия информации с определенного канала.

Волоконно-оптическая связь находит все более широкое применение во всех областях — от компьютеров и бортовых космических, самолётных и корабельных систем, до систем передачи информации на большие расстояния. Результатом стало создание трансокеанских и трансконтинентальных линий связи протяженностью в десятки тысяч километров. Кроме того, увеличивается число оптических каналов передаваемых по одному волокну методом волнового уплотнения.

Ранее считалось, что волоконно-оптические системы передачи (ВОСП) обладают повышенной скрытностью, однако всегда существует принципиальная возможность съёма информации, передаваемой по оптическим каналам связи.

Изгиб волокна.

При данном методе подключения, кабель разбирается до волокна и изгибается под определенным радиусом. При сгибании волокна, оно искривляется таким образом, чтобы угол отражения стал меньше чем критический, и свет начал проникать через оболочку. Очевидно, что могут быть два типа сгибов: микросгиб и макросгиб.

Оптическое расщепление с использованием сплиттера, который отводит часть оптического сигнала. Этот метод является интрузивным, поскольку требует разрезания волокна, что вызовет срабатывание тревоги. Однако, необнаруженное подключение такого типа может работать годами.

Использование связанных волн.

Данный способ используется для перехвата сигнала от волокна-источника в волокно-приемник посредством аккуратной полировки оболочек до поверхности ядра и затем их совмещения. Это позволяет некоторой части сигнала проникать во второе волокно. Данный способ трудновыполним в полевых условиях.

V-образный вырез.

V-образный вырез – это специальная выемка в оболочке волокна близкая к ядру, сделанная таким образом, что угол между светом, распространяющимся в волокне и проекцией V-выреза больше, чем критический. Это вызывает полное внутреннее отражение, при котором часть света будет уходить из основного волокна через оболочку и V-образный вырез.

Выше приведенные методы работают, когда по волокну передается один канал, т.е. в системах без волнового уплотнения (DWDM). В системах с волновым разделением каналов в волокне передается до 250 каналов. Поэтому целью данной работы является оценка возможности использования акустооптического эффекта для доступа к одному из передаваемых каналов.

На ядре волокна создается решетка Брэгга, с ее помощью достигается отражение части сигнала с волокна. Это достигается наложением и интерференцией УФ лучей, создаваемых лазером с УФ возбуждением.

Под воздействием акустической волны в сердцевине оптоволокна создаётся дифракционная решётка периодического изменения показателя преломления. При взаимодействии с дифракционной решеткой, оптическая волна отклоняется от своего первоначального направления, и часть её выходит за пределы ОВ. Физическим явлением, описывающим данный процесс, является дифракция Брэгга на высокочастотном звуке (>10 МГц), длина волны Λ которого удовлетворяет условию: $(\lambda L/\Lambda 2)>1$, где λ – длина волны электромагнитного излучения, L - ширина области распространения звуковой волны. Деформации, создаваемые упругой волной, формируют периодическое изменение показателя преломления внутри оптоволокна, которое для света является дифракционной решёткой (рис.1).

Максимальный угол отклонения единственного наблюдаемого дифракционного максимума равен двум углам Брэгга ($2\theta_B = 2\lambda/n_1\Lambda$). Частота отклонённой электромагнитной волны приблизительно равна частоте основного информационного потока. Интенсивность дифракционного максимума может быть определена по формуле:

$$I = I_0 \sin^2\left(\frac{\pi}{2}\sqrt{J_0 M_2}\,\frac{L}{\lambda}\right),$$

где J_0 – интенсивность звуковой волны,
M2=1,51×10-15 сек3/кг - акустооптическое качество кварца.

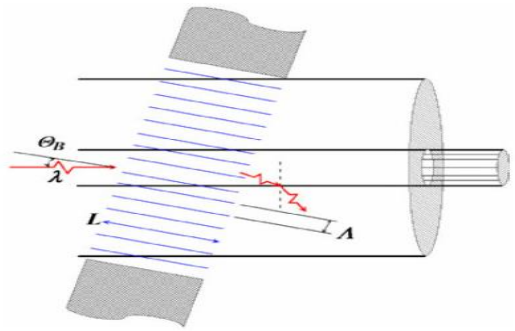


Рисунок 1 – Формирование дифракционной решетки в сердцевине оптоволокна акустической волной.

Вычисления показывают, что для многомодового оптоволокна с параметрами (d/D)=(50/125) при акустическом воздействии с длиной волны звука Λ=10 мкм и длине взаимодействия L=10-3 м, максимальный угол отклонения от первоначального направления распространения составляет 5 градусов.

График зависимости интенсивности первого дифракционного максимума от интенсивности звуковой волны представлен на рисунке 2. Из графика видно, что даже при невысоких интенсивностях звуковой волны выводимое оптическое излучение достаточно велико для регистрации его современными фотоприёмниками. При фиксированной интенсивности звука, путём изменения области озвучивания L можно добиться максимального значения интенсивности в дифракционном максимуме, тем самым увеличить интенсивность света отводимого в канал утечки.

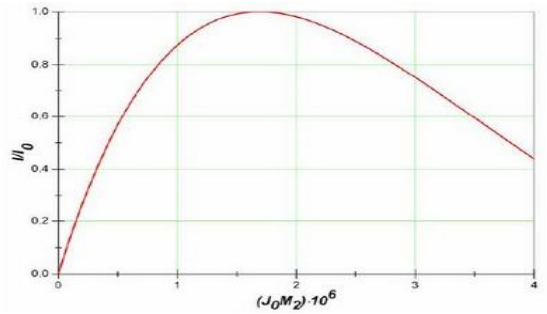


Рисунок 2 – Зависимость интенсивности дифракционного максимума от интенсивности звуковой волны.

Изменяя частоту акустического сигнала можно выбирать номер контролируемого канала в многоволновом сигнале передаваемого в волоконном световоде. Метод снятия информации состоит в регистрации отведенного излучения путем фокусировки с помощью пассивных оптических элементов (линз, призм) и направлением его на фотодетектор.

Для реализации данного метода необходимо наличие акустического генератора и напыления электродов на волоконный световод для формирования звуковой волны требуемого уровня и устройств фокусировки снятого оптического излучения.

Подводя итог необходимо отметить, что для формирования устойчивой дифракционной решетки необходимо снятие защитных покровов с волоконного световода и напыления электродов. Кроме того, требуется применение фокусировки сигнала для эффективного сбора излучаемой энергии.

***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).

СМЯГЧЕНИЕ ПИЛОТНОГО ЗАГРЯЗНЕНИЯ ЧЕРЕЗ КОНФИГУРАЦИЮ АНТЕННЫ БАЗОВОЙ СТАНЦИИ В WCDMA

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

Сакович Д.А.
Аксёнов В.А. – старший преподаватель

В этой работе цель состоит в том, чтобы оценить, сколько пилотно загрязненных территорий можно уменьшить с помощью традиционного метода планирования радиосети как выбор диаграммы направленности и наклона антенны.

Пилотное загрязнение наблюдается в районах, где мобильным станциям не хватает RAKE для обработки всех принятых пилот-сигналов или в них отсутствует доминирующий пилот-сигнал. Эта работа оценивает влияние конфигурации антенны базовой станции в 3-х секционных и в 6-ти разных WCDMA сайтах на количество пилотно загрязненных территорий. В WCDMA (широкополосный множественный доступ с кодовым разделением) система как UMTS (универсальная мобильная система связи), мобильные телефоны в сети могут идентифицировать различные сектора базовой станции в соответствии с их основным общим канальным пилот-сигналом (P-CPICH) [1]. Сигнал CPICH является предопределенной последовательностью символов, и она используется в качестве эталона для других общих физических каналов нисходящей линии связи. Более того, это рассматривается как чисто физический канал, поскольку он не несет данных. CPICH используется для принятия решений о передаче обслуживания (handover), выборе сот и повторные выборы, и, при некоторых обстоятельствах, чтобы помочь в канале предварительный расчет. Достижение достаточного покрытия CPICH важно, чтобы обеспечить надлежащую функциональность выбора ячеек и повторный выбор, и измерения передачи. Тем не менее, CPICH также потребляет ограниченную мощность передачи из-за того, что базовые станции отправляют свои уникальные CPICH сигналы непрерывно. Следовательно, распределение мощности CPICH является одной из важных задач в планировании сети WCDMA. На практике, однако, покрытие CPICH должно перекрываться в пограничных зонах сот для возможности мягких хэндоверов (SHO) и в для того, чтобы добиться надлежащего внутреннего покрытия на границах ячейки (рис. 1) [1].

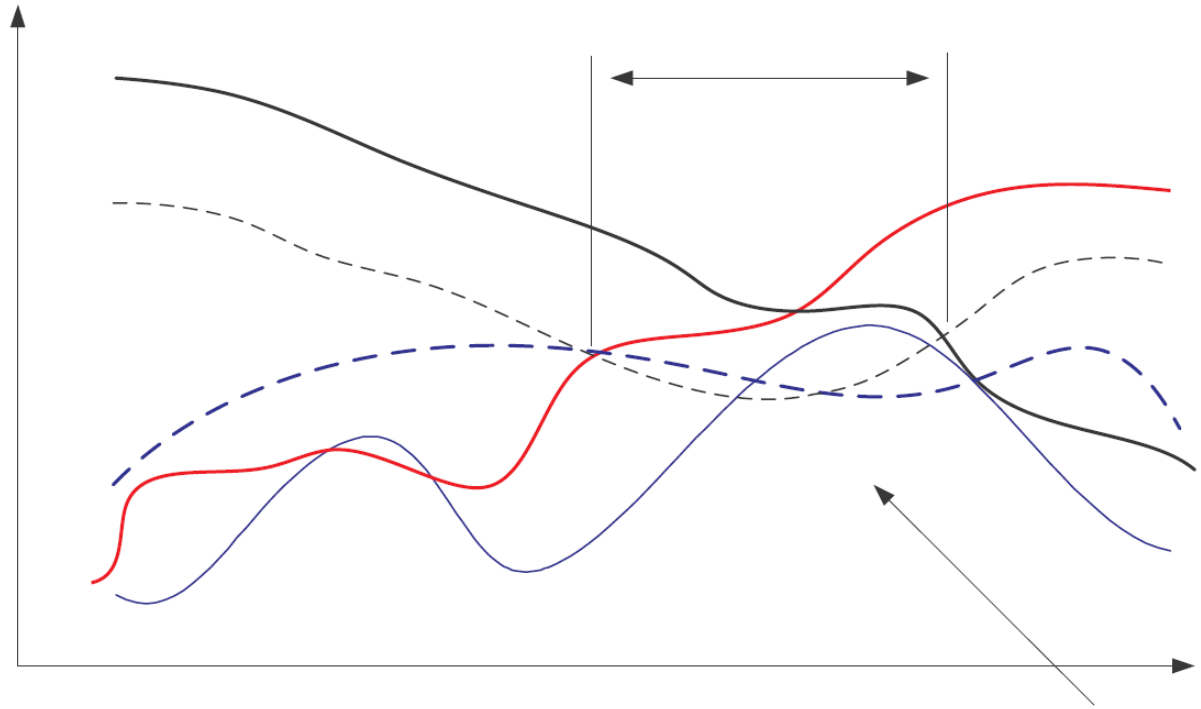


Рис 1. – Пример мягкого хэндовера

Пилотное загрязнение наблюдается в районах, где много сигналов CPICH (разные сигналы CPICH или их многолучевые компоненты), полученные на RAKE приёмник мобильной станции, чем он способен обрабатывать, или ни один из полученных сигналов CPICH достаточно доминирующий [2]. Каждая сота, которую слышит мобильный телефон, практически увеличит уровень помех в нисходящей линии связи (DL). Таким образом, слушая ненужные пилотные сигналы снижается

принимаемая энергия на чип по удельной мощности (Ec / N0) от обслуживающей соты; другими словами, уменьшает качество существующего соединения. Чтобы избежать пилотно загрязненных участков, зоны доминирования сот должны быть по возможности чистыми и ненужные сигналы CPICH не должны быть услышаны. Тем не менее, пилотного загрязнения нельзя полностью избежать традиционными методами планирования радиосети из-за неоднородной среды распространения и перекрытия сот.

В общем, помехи от пилотного загрязнения могут быть уменьшены оптимизацией мощности пилотного сигнала автоматически таким образом, чтобы требуемые пороги покрытия все еще превышены. Простым методом управления мощностью CPICH, производительность радиоинтерфейса сети WCDMA может быть немного улучшена. Реализация репитеров может также уменьшить помехи от пилотных помех в сетях CDMA. Очевидно, что ретрансляторы способны уменьшить пилотные загрязненные районы сделать область доминирования донорских клеток более четкой, тем самым уменьшая вклад мешающих пилотов. Однако ретрансляторы могли сдвинуть помехи от пилотного загрязнения от доминированной области ретрансляторов, создавая территорию пилотных загрязнений в другом месте.

В этой работе, количество пилотных загрязненных территорий было изучено в сотовой сети WCDMA с разными сценариями секторов, диаграммы направленности антенны, направления и наклон антенны. Результаты показывают, что пилотные загрязненные районы можно уменьшить, выбрав подходящую конфигурацию антенны базовой станции. Диаграмма направленности антенны и направление антенны также имеет явное влияние на пилотное загрязнение. Кроме того, наклон антенны влияет на пилотно загрязненные районы.

Список использованных источников:

1. Дж. Лайхо, А. Вакер, Т. Новосад (ред.), Планирование и оптимизация радиосети для UMTS. Чичестер: John Wiley & Sons Ltd, 2002.

2. Дж. Лемпиайнен, М. Маннинен (ред.), Планирование, оптимизация и управление QoS UMTS радиосети. Дордрехт: Kluwer Academic

INTRANET VPN

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

Журович А.С.

Лагутин А.Е. – к.т.н.

Бурное развитие интернета и появление новых технологий ставят под угрозу безопасность конфиденциальных данных, хранящихся на компьютерах пользователей. Особенно это актуально в сетях с большим количеством пользователей, использующих интернет. Контролировать каждый узел отдельно довольно проблематично и неэффективно в свете того, что каждый пользователь компьютера индивидуален и использует различные сайты. Ситуация усложняется когда появляется потребность обмениваться конфиденциальными данными за пределами локальной сети. Эти проблемы решаются при помощи Intranet VPN (Virtual Private Network). Не смотря на слово «Private» в названии технологии, существует возможность организации и общедоступных – нешифрованных сетей. Вообще, организация VPN может осуществляться огромным количеством способов с использованием разных технологий (SSL VPN, IPSec, GRE и др.).

VPN позволяет объединить удалённые локальные сети либо присоединить отдельные узлы к одной подсети (рисунок 1). При этом трафик, проходящий через интернет, зашифрован и при прохождении через VPN-сервер может фильтроваться, анализироваться, ограничиваться и т.д. при наличии соответствующего программного обеспечения. Благодаря этому упрощается задача контролирования не только сети в целом, но и каждого отдельного пользователя. Для подобных целей существует такие комплексные решения как Kerio Control, которое мы и возьмём в качестве примера.

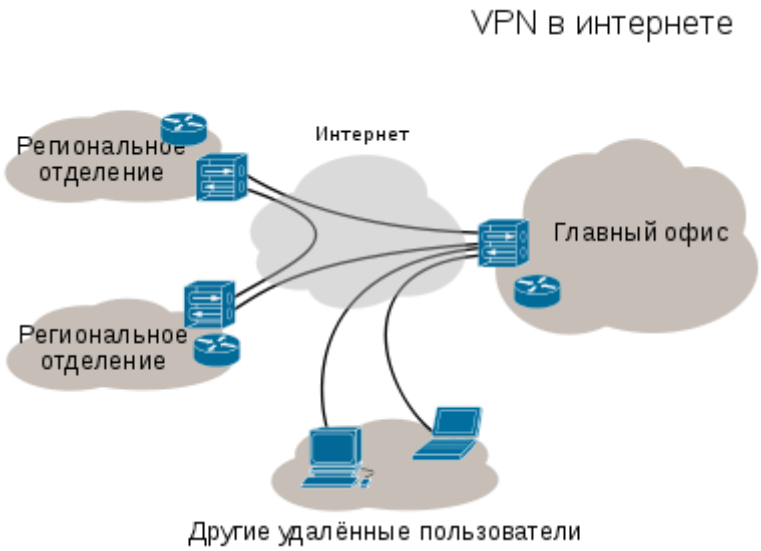


Рис. 1 – Упрощённая структура VPN

Данное решение включает в себя, кроме собственного VPN, межсетевой экран, контроль пропускной способности канала, IPsec VPN, мониторинг трафика, интегрированный антивирус и т. д. Данный перечень компонентов достаточен для защиты от большинства современных угроз и безопасной передачи конфиденциальных данных между пользователями.

Реализация подобных программных комплексов уместна для относительно небольших предприятий и малых офисов, которым не выгодно вкладывать средства в покупку отдельно выделенного сервера, выполняющего все представленные функции, при уже имеющемся сервере, у которого есть нереализованные вычислительные мощности.

Список использованных источников:
1. Kerio Control http://www.kerio.ru/products/kerio-control
2. Принципы организации VPN http://ciscotips.ru/vpn

РЕЖИМЫ СОХРАНЕНИЯ ЭНЕРГИИ В NB-IOT

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

Каптюг Д. А.
Аксенов В. А. – старший преподаватель

В данной работе будут подробно рассмотрены режимы энергосбережения PSM и eDRX для технологии NB-IoT.

Инновационной технологией Интернета вещей является решение узкополосного IoT (Narrow-Band IoT или NB-IoT). Это технология сотовой связи на основе LTE, предназначенная для стационарных устройств с низкими объемами передаваемых данных и малым потреблением энергии (Low Power Wide Area, LPWA). В данной работе подробно рассмотрено как в технологии NB-IoT реализованы бесперебойная передача данных и низкое энергопотребление**.**

NB-IoT учитывает такие специфические потребности как улучшенная чувствительность к модуляции сигнала для подключения сотен тысяч устройств. Также для работы с NB-IoT не нужна SIM-карта и достаточно небольшой мощности приемопередатчика, таким образом устройства IoT могут работать много лет от одной батарейки. Таким устройствам важно потреблять как можно меньше энергии. Для этого в NB-IoT предусмотрены два режима энергосбережения: Power Saving Mode (PSM) и Extended idle mode DRX (eDRX). Рассмотрим их подробнее.

Режим сохранения энергии PSM, Power Saving Mode. Согласно спецификации 3GPP TS 23.682, Power Saving Mode (PSM) – это режим является аналогичный отключению питания, при котором устройство остается зарегистрированным в сети. Любопытно, что режим PSM появился в спецификациях 3GPP раньше, чем NB-IoT – в 3GPP Release 12.

Устройство NB-IoT инициирует режим PSM, включая значения двух таймеров в запросы ATTACH REQUEST/TAU REQUEST, посылаемые в процедурах Attach и TAU (TAU, Tracking Area Update — это периодическая процедура, которая используется в LTE для уведомления сети о доступности и местоположении мобильного устройства).

Первый таймер — T3324 Active Timer — определяет время, в течение которого устройство остается доступным со стороны сети после процедуры Attach, TAU или передачи данных, а второй таймер — T3412 Extended periodic TAU Timer — определяет период процедуры TAU.

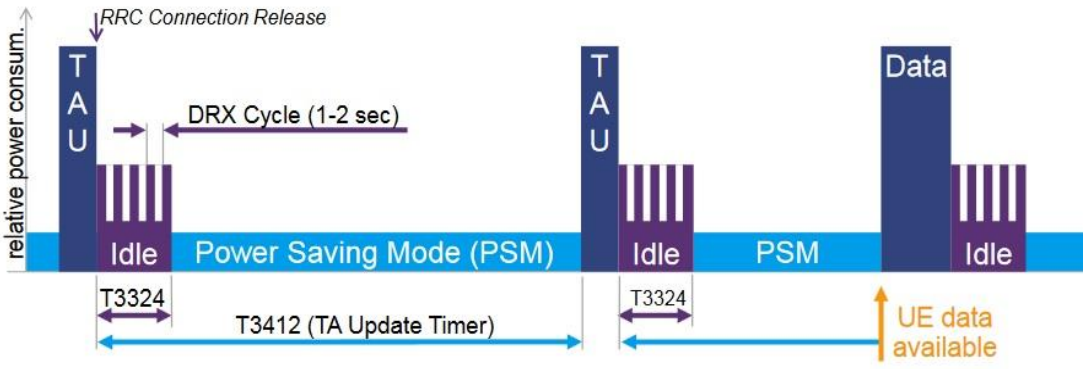


Рисунок 1 – Режим PSM и таймеры T3324, T3412

Если сеть разрешает использовать PSM, то значения этих таймеров включаются в ответные сообщения ATTACH ACCEPT/TAU ACCEPT. При определении значений таймеров сеть может принимать во внимание не только значения, запрашиваемые устройством, но и локальную конфигурацию. Другими словами, сеть не обязана подтверждать в точности те значения таймеров, которые запросило устройство. Зато устройство обязано применить значения, полученные от сети.

Период нахождения устройства в режиме PSM определяется как разница между Extended periodic TAU Timer и Active Timer (T3412-T3324). Так как значение T3324 Active Timer может быть равно нулю, то максимальное теоретическое время нахождения устройства в режиме PSM равняется максимальному времени T3412 Extended periodic TAU Timer и составляет 413 дней и 8 часов. Максимальное значение T3324 Active Timer составляет 3 часа и 6 минут (186 минут).

Когда устройство находится в режиме PSM, оно недоступно со стороны сети (для так называемых mobile terminating сервисов). GSMA рекомендует операторам сотовой связи сохранять и передавать устройству (после выхода последнего из режима PSM) как минимум последний пакет

данных длительностью 100 бит. Устройство может выйти из режима PSM в любое время (например, если устройству нужно срочно передать какие-нибудь данные, как на картинке выше).

Режим сохранения энергии eDRX (Extended idle mode DRX). eDRX (Extended idle mode DRX) считается дополнительным режимом энергосбережения устройства, он появился в спецификациях 3GPP Release 13. DRX означает прерывистый приём (Discontinuous Receiving). Метод прерывистого приема известен в сотовой связи заключается в том, что для сохранения энергии приемный тракт устройства включается периодически в определенные промежутки времени, а большую часть времени отключен. Сеть «знает» об этом и посылает сигналы вызова (paging) только в «правильные» моменты времени. Расширенный режим прерывистого приёма (eDRX) позволяет существенно увеличить период времени, когда приемный тракт устройства выключен. Согласно спецификации 3GPP TS 23.682, период прерывистого приема eDRX в режиме NB-IoT составляет от 20,48 до 10485,76 секунды (10485 секунд — это почти 3 часа).

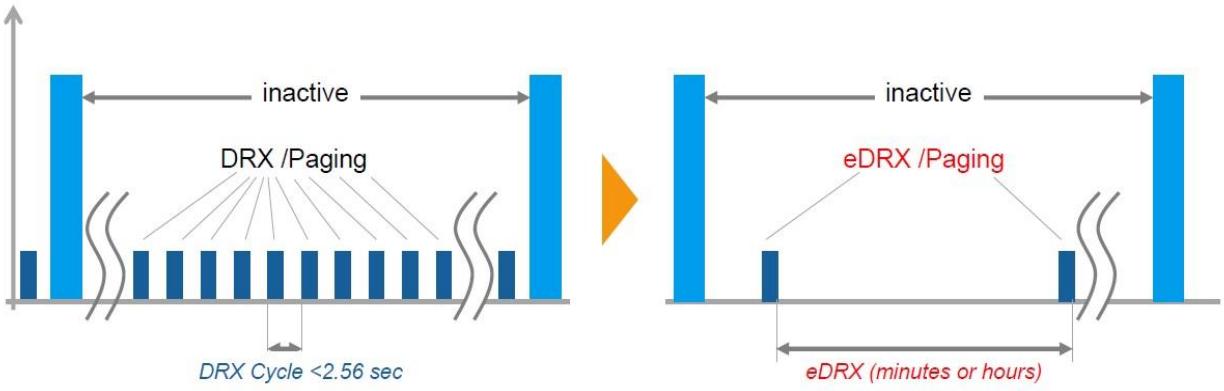


Рисунок 2 – Сравнение «старого» DRX и «нового» eDRX

Устройство NB-IoT активирует режим eDRX, передавая значение длительности периода eDRX в запросах ATTACH REQUEST/TAU REQUEST, посылаемых в процедурах Attach и TAU. Если сеть позволяет использование режима eDRX, то значение периода eDRX включается в ответные сообщения ATTACH ACCEPT/TAU ACCEPT. Сеть не обязана подтверждать запрошенное устройством значение периода eDRX, а вот устройство обязано применить значение, переданное сетью.

Как и в случае с PSM, при использовании режима eDRX GSMA рекомендует операторам сохранять и передавать устройству как минимум последний пакет данных длительностью 100 бит. Режим eDRX может применяться одновременно с режимом PSM.

Режимы PSM и eDRX входят в число минимальных требований к сетям NB-IoT, рекомендованных GSMA.

Список использованных источников:

1. Тихвинский В.О., Бабин А.И. и Бочечка Г.С., Сети IoT/M2M: технологии, архитектура и приложения.
2. Hossam Fattah, 5G LTE Narrowband Internet of Things (NB-IoT)
3. Тихвинский В.О., Терентьев С.В. Высочин В.П. Сети мобильной связи LTE/LTE Advanced: технологии 4G, приложения и архитектура. – М.: Медиа-Паблишер, 2014.
4. Trend and Status of NB-IoT protocol in LTE-A. – Taiwan Association of Information and Communication Standards, 2016.

МОДЕЛИРОВАНИЕ ТРАКТА ВЫСОКОСКОРОСТНОЙ ОПТИЧЕСКОЙ СИСТЕМЫ ПЕРЕДАЧИ

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

Мойсиевич Ю.С.

Тарченко Н.В. – к.т.н., доцент

На современном этапе развития систем связи происходит повсеместное внедрение волоконно-оптических систем передачи (ВОСП), Суммарная пропускная способность современных высокоскоростных линий связи со спектральным уплотнением каналов может составлять десятки Тбит/с, поэтому наиболее актуальной стоит задача проектирования и моделирования ВОСП.

Целью исследовательской работы является разработка математической модели и последующее моделирование высокоскоростного оптического тракта с различными способами построения. Особое внимание уделено способам детектирования оптического сигнала и оценке отношения оптического (ООСШ) и электрического (ЭОСШ) отношения сигнал/шум для обеспечения заданной вероятности ошибки [1].

Способы организации передачи информации по оптическому волокну многообразны и постоянно совершенствуются. Существенную помощь при их изучении и моделировании оказывает классификация. В результате проведения библиографического поиска и анализа литературы предложена классификация ВОСП по основным классификационным признакам (тип передаваемого сигнала, способ модуляции, метод уплотнения, способ приема, протяженность), с помощью которых можно описать любую проектируемую либо эксплуатируемую систему передачи.

Для различных способов детектирования сигнала проведена оценка ЭОСШ на выходе приемника, для чего рассмотрен расчет полезного сигнала $P_{С\,вых}$ и полного шума $P_{Ш}$ [2, 3]. В результате получены математические выражения для расчета теоретического предела ЭОСШ, когда шумами можно пренебречь (таблица 1).

Таблица 1 – Мощность полезного сигнала и ЭОСШ на выходе фотодетектора

Параметр	Непосредственный прием	Когерентный прием	
		Гетеродинный	Гомодинный
$P_{С\,вых}$	$\left(MS_i\right)^2 P_{С\,вх}^2 R_{Н}$	$2\left(MS_i\right)^2 P_{С\,вх} P_0 R_{Н}$	$4\left(MS_i\right)^2 P_{С\,вх} P_0 R_{Н}$
ЭОСШ$_{max}$	$\frac{\eta P_{С\,вх}}{2h\nu_С M^x B}$	$\frac{\eta P_{С\,вх}}{h\nu_С M^x B}$	$\frac{2\eta P_{С\,вх}}{h\nu_С M^x B}$

В таблице приняты следующие обозначения: M – коэффициент лавинного умножения или внутреннего усиления фототока; S_i – токовая чувствительность фотодиода, А/Вт; $P_{С\,вх}$ – мощность оптического сигнала, поступающего на вход приемника, Вт; P_0 – мощность сигнала гетеродина, Вт; $R_Н$ – нагрузочное сопротивление фотодетектора, которое зависит от полосы частот принимаемого сигнала и от схемы реализации оптического приемника, Ом; M^x – коэффициент избыточного шума лавинного умножения, B – полоса пропускания выходного фильтра оптического приемника, Гц; η – квантовая эффективность; $\nu_С$ – частота оптической несущей, Гц;

Как видно из таблицы, гетеродинный прием обеспечивает выигрыш в 2 раза по сравнению с непосредственным приемом, а гомодинный – в 4 раза. В случае использования балансного приемника можно получить дополнительный выигрыш до 3 дБ. Предложенные модели позволяют при проектировании цифровых ВОСП оценить с учетом вида модуляции параметры оптических приемников и выбрать наилучший метод приема, при котором обеспечивается требуемое качество при максимальной чувствительности, что обеспечивает максимальную протяженность участка регенерации в системах со спектральным разделением каналов.

По линейному тракту ВОСП проведена оценка ООСШ с учетом шумов и параметров элементов системы передачи (источников оптического излучения, терминальных мультиплексоров и мультиплексоров ввода/вывода, оптических усилителей, компенсаторов дисперсии). Это позволяет оценить длину регенерационного участка при заданных характеристиках оборудования либо выбрать оборудование с такими параметрами, которые обеспечат максимальную длину участка и необходимое качество услуг.

Список использованных источников:

1. Леонов А. В., Наний О. Е., Слепцов М. А., Трещиков В. Н. Тенденции развития оптических систем дальней связи; в журнале Прикладная фотоника, том 3, № 2, 2016 – с. 123-145.

2. Фокин В. Г. Когерентные оптические сети : Учебное пособие / Сибирский государственный университет телекоммуникаций и информатики; каф. многоканальной электросвязи и оптических систем. – Новосибирск, 2015. – 372 с.

3. Соломенчук В. Д., Мищенко В. А., Гура К. Н. Оптические транспортные сети. – Киев: Центр последипломного образования ПАО «Укртелеком», 2014 – стр. 294.

ИСКАЖЕНИЯ И СПОСОБЫ ИХ МИНИМИЗАЦИИ

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

Захарченя А.С., Шевченко Т.Б.

Печень Т.М.. – старший преподаватель

Работа посвящена исследованиям линейных и нелинейных искажений в системах инфокоммуникаций. Показано от каких характеристик зависит уровень искажений. Приведены способы минимизации их влияния с использованием корректоров.

В реальных системах инфококоммуникаций возникают искажения и помеховые ситуации [1]. В результате их воздействия сообщение может воспроизводиться с некоторой ошибкой. Идеализированный случай представляет собой систему, при прохождении которой выходной сигнал не содержит нежелательных искажений и является точной копией входного.

Системы инфококоммуникаций описываются характеристиками: амплитудно-частотной (АЧХ) и фазочастотной (ФЧХ), амплитудной характеристики (АХ), характеристикой группового времени запаздывания (ХГВЗ) и др. [2]. В идеальном случае АЧХ должна иметь постоянное значение, т.е. система все гармонические составляющие должна передавать с одинаковым усилением или ослаблением; ФЧХ же должна быть линейной. Условие линейности ФЧХ исходит от того, что производная от этой функции определяет задержку составляющих сигнала различной частоты (групповое время задержки). Данная характеристика называется ХГВЗ. Сравнение идеального и реального АЧХ приведено на рисунке 1 на примере фильтра нижних частот (ФНЧ).

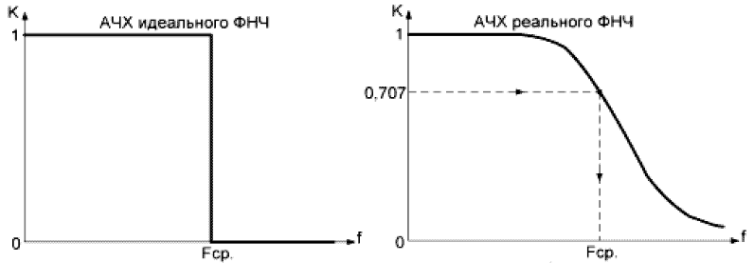


Рисунок 1 – Амплитудно-частотная характеристика различных фильтров нижних частот

ХГВЗ рассчитывается по формуле:

$$\tau(\mathrm{f}) = -\frac{d\varphi(f)}{df}, \tag{1}$$

Если ФЧХ нелинейна и представляется в виде ряда Тейлора с произвольными коэффициентами a_i, то ХГВЗ примет следующий вид:

$$\tau(\mathrm{f}) = -(a_1 + a_2 * f_2 + \ldots + a_i * f_i), \tag{2}$$

Как видно из уравнения, ХГВЗ равно постоянной величине. Изменение характеристик могут вызывать отраженные от элементов схем сигналы (электрическое эхо). Следует отметить, что неравномерности АЧХ и ФЧХ приводит к возникновению линейных искажений. Их влияние можно скомпенсировать при помощи корректирующих цепей (корректор ХГВЗ и предыскажающий контур).

Нелинейные искажения возникают из-за нелинейности АХ (характеристики зависимости выходной мощности от входной) усилителей и других устройств трактов. На данной характеристике можно выделить линейный, квазилинейный и нелинейный участки. В случае работы в линейном участке никаких искажений не происходит, однако в случае превышения допустимых значений мощности устройство переходит в нелинейный участок или участок насыщений, что сопровождается возникновением дополнительных гармонических составляющих. Это можно объяснить следующим образом. Пусть АХ аппроксимируется рядом Тейлора, тогда при входном гармоническом колебании его степень будет порождать гармоники соответствующего порядка. Худшим случаем является присутствие на входе линии смеси сигналов, что приводит к возникновению комбинированных составляющих.

В заключении отметим, что, рассмотрев основные виды искажений систем инфокоммуникаций, выяснили их прямое влияние на такие параметры как скорость и отношение сигнал-шум. Таким образом, коррекция искажений обязательна для обеспечение требуемого качества связи.

Список использованных источников:

1. Баскаков С.И. Радиотехнические цепи и сигналы / С.И. Баскаков. – Москва: «Высшая школа», 2000. – 459 с.
2. Клюев Л.Л. Теория электрической связи / Л.Л. Клюев – Минск: Новое знание ; М. : ИНФРА-М, 2016 – 448 с.

ПРИМЕНЕНИЕ MIMO ТЕХНОЛОГИИ В МОБИЛЬНЫХ СИСТЕМАХ ШИРОКОПОЛОСНОГО РАДИОДОСТУПА

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

Трофимик Я.В.

Печень Т.М. – старший преподаватель

В работе рассмотрены преимущества мобильных систем широкополосного радиодоступа, построенных с применением MIMO технологии. Приведено краткое сравнение сетей 3G и 4G.

Мобильная трансляция цифрового потока LTE напрямую относится к новым разработкам 4G. Взяв для анализа 3G сеть, можно обнаружить, что ее скорость передачи данных в 11 раз меньше, чем 4G. Все же скорость, как получения, так и трансляции данных LTE нередко бывает плохого качества. Связано это с нехваткой мощности или уровня сигнала, который получает модем 4G LTE от станции. Каждый современный человек рано или поздно сталкивается с проблемой низкого качества мобильного интернета и возникает вопрос, а как улучшить качество беспроводного интернета и возможно ли на это влиять.

Для существенного улучшения качества распространения информации внедряют антенны 4G MIMO. MIMO (Multiple Input Multiple Output – множественный вход и множественный выход) – метод пространственного кодирования сигнала, позволяющий увеличить полосу пропускания канала, при котором для передачи данных используются две и более антенны и такое же количество антенн для приёма. На рисунке 1 показано, что передающие и приёмные антенны разнесены настолько, чтобы достичь минимального взаимного влияния друг на друга между соседними антеннами.

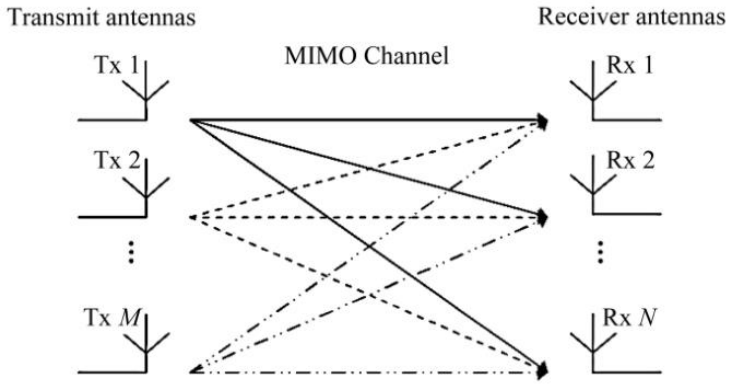


Рисунок 1 – Приемопередающая система MIMO технологии

Суть технологии такова: методом пространственного кодирования сигнала увеличивается полоса пропускания канала, в котором передача данных происходит через некоторое число антенн. Простыми словами: происходит расширение сигнала за счет увеличения количества параллельных антенн. Это позволяет существенно улучшить пропускную способность сигнала, не прибегая к расширению полосы. Антенна MIMO способна транслировать информацию по нескольким каналам с незначительной задержкой. Информация предварительно кодируется, а затем восстанавливается на приемной стороне. В итоге не только увеличивается скорость распределения данных, но и значительно улучшается качество сигнала. MIMO дает шансы увеличить скорость трансляции сигнала более чем в два раза. Достигается это благодаря монтажу в коробе сразу нескольких антенн, которые располагают на незначительном удалении одна от другой. Одновременное получение, а также раздача цифрового потока антеннами к получателю происходит через два независимых кабеля. Это позволяет существенно увеличить скоростные параметры. MIMO применяется успешно в таких беспроводных системах, как WiFi, а также сотовые сети и WiMAX. Применение этой технологии, имеющей, как правило, два входа и два выхода, позволяет улучшить спектральные качества WiFi, WiMAX, 4G/LTE и прочих систем, поднять скорость передачи информации и емкость потока данных. Перечисленные достоинства достижимы благодаря трансляции данных от 4G антенны MIMO к получателю посредством нескольких беспроводных соединений.

В заключение можно сделать вывод, что MIMO оправдала себя как перспективная технология для построения мобильных систем широкополосного радиодоступа со скоростями в сотни Мб/с.

Список использованных источников:

1. Сайт Экопарк Z [Электронный ресурс] – Режим доступа : http://ep-z.ru/
2. Сайт компании Антенна 31 [Электронный ресурс] – Режим доступа: http://antenna31.ru/

ЭФФЕКТИВНОСТЬ РАЗЛИЧНЫХ ВИДОВ МОДУЛЯЦИЙ В ВОСП

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

Червяков А.И.

Урядов В.Н. – к.т.н.,доцент

В настоящее время интенсивно развиваются исследования в области новых типов модуля- ции 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 еди- ницы передаваемой информации.

Эффективность и помехоустойчивость ВОСП в значительной мере зависит от используемых методов оптической модуляции. Эффективность ВОСП подразумевает более эффективное использование спектральных каналов в системах плотного волнового мультиплексирования (DWDM), а повышение помехоустойчивости заключается в снижении чувствительности оптических сигналов к искажениям из-за дисперсии или нелинейности.

В оптическом диапазоне электромагнитных волн могут быть реализованы следующие методы модуляции: амплитудная модуляция, частотная, фазовая, поляризационная, модуляция интенсивности. Кроме того, возможны различные комбинационные виды модуляции с одновременно управляемым изменением сразу нескольких параметров. Первые три простых способа модуляции, а также все комбинационные применяются в ВОЛС менее широко, чем модуляция по интенсивности и относительная фазо- вая модуляция (DPSK)

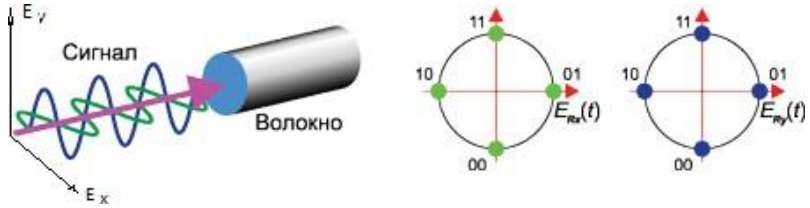


Рис. 1. Структура оптического сигнала при использовании DP-QPSK

При DP-QPSK используются 2 поляризации и 4 фазы сигнала (M=4), при которой фаза высокочастотного колебания может принимать 4 различных значения с шагом, кратным π / 2 .

Из рис. 1 видно, что соответствие между значениями символов и фазой сигнала установлено таким образом, что в соседних точках сигнального созвездия значения со- ответствующих символов отличаются лишь в одном бите. При передаче в условиях шума наиболее вероятной ошибкой будет определение фазы соседней точки созвездия. При указанном кодировании, несмотря на то, что произошла ошибка в определении значения символа, это будет соответствовать ошибке в одном (а не двух) бите информации. Таким образом, достигается снижение вероятности ошибки на бит. Указанный способ кодирования называется кодом Грея.

Следует иметь в виду, что в оптических системах связи все фазовые форматы модуляции используют дифференциальные фазовые методы, так как в оптическом диа- пазоне практически нецелесообразно выделять абсолютное значение фазы несущей световой волны принимаемого сигнала. Поэтому информация закладывается в относи- тельный сдвиг фазы несущих двух последовательных импульсов.

Когерентное детектирование и формат DP-QPSK предоставили исключительно надёжную технологическую платформу для создания DWDM-систем связи с канальной скоростью 100 Гбит/с, а само применение рассматриваемого формата модуляции по- зволяет увеличить в 4 раза спектральную эффективность передачи информации.

Список использованных источников:

1. Интернет-энциклопедия: Методы оптической модуляции. [Электронный ре- сурс]. – Режим доступа: www.rp-photonics.com. – Дата доступа: 24.03.2019.

2. Журнал «t8»: Когерентные DWDM-системы. [Электронный ресурс]. – Режим доступа: http://t8.ru/?page_id=3981. – Дата доступа: 24.03.2019.

3. Meghan Fuller Hanna // Lightwave. 2008. November 1. «Is DP-QPSK the end- game for 100 Gbits/sec».

МАГИСТРАЛЬНАЯ СЕТЬ ПЕРЕДАЧИ ДАННЫХ ОПЕРАТОРА СВЯЗИ

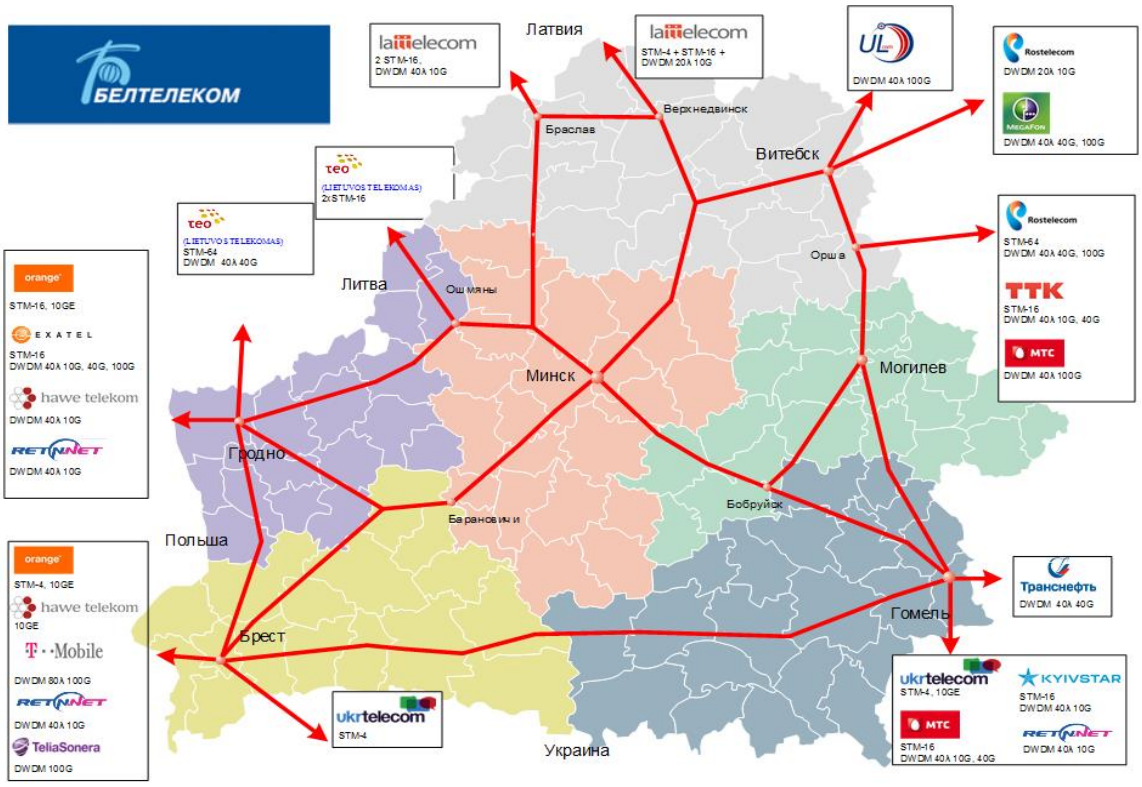
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Глушкевич Е.В.

Тарченко Н.В.

Высокий темп роста пользования услугами сети Интернет является предпосылкой к повсеместному развитию сетей передачи данных.

Сеть передачи данных – сеть электросвязи, которая предназначена для целей приема, передачи, обработки, хранения данных и сообщений электросвязи (включая телефонные вызовы, телеграфные сообщения, служебные и информационные сообщения, сетевые пакеты сетей передачи данных) без ограничений по используемым пользовательским, транспортным и сетевым протоколам передачи данных, за исключением сетей электросвязи, реализующих предоставление услуг эфирной трансляции телевизионных и звуковых программ, спутниковой электросвязи [1]. Структура магистральной сети передачи данных представлена на рисунке, эта сеть обеспечивает передачу данных между всеми областными центрами РБ [2].



В настоящее время магистральная сеть передачи данных РБ модернизируется путем перехода к технологии DWDM/OTN. Преимуществами использования такой технологии являются:

- увеличение пропускной способности (до 80 длин волн в одном оптическом волокне со скоростью передачи данных 100 Гбит/с на одной длине волны);
- возможность передачи разнородного трафика на одной длине волны (телефонии и передачи данных);
- возможность масштабирования сети путем расширения емкости;
- высокая надежность за счет встроенных механизмов мониторинга;
- передача больших объемов информации на дальние расстояния (до сотен километров) без регенерации.

Сеть DWDM/OTN является высокоскоростной магистральной сетью передачи данных и представляет собой фундамент для строительства магистральной передачи данных IP/MPLS, а также обеспечивает транзит трафика через Республику Беларусь. Узлы сети DWDM/OTN располагаются в областных и районных центрах Республики Беларусь.

Список использованных источников:
1. Закон Республики Беларусь «Об электросвязи» от 19 июля 2005.
2. Транспортная сеть Республики Беларусь - https://beltelecom.by/about/communication-networks/primary-network.

МОБИЛЬНОЕ ПРИЛОЖЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ МЕРОПРИЯТИЯМИ

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

Зубко А.Е.

Чепикова В.В. – ассистент, магистр технических наук

Введение

Смартфоны за последнее десятилетие стали неотъемлемой частью жизни большинства людей на Земле, их популярность обусловлена широкой функциональностью, доставшейся от их старшего брата - карманного персонального компьютера. Смартфоны отличаются от обычных мобильных телефонов наличием достаточно развитой операционной системы, открытой для разработки ПО сторонними разработчиками, и, в следствие чего, широким выбором мобильных приложений самых различных категорий. Приложение, которое мы будем рассматривать в этом докладе, относится к категории клиентов для веб-сервисов. Существование такого рода приложений обязано инструментам из области сетевых технологий, появившихся уже более 25-ти лет назад и использующихся и по сей день - а именно появлению HTTP.

Особенности рассматриваемой системы

Рассматриваемое приложение является частью тонкого клиента для веб-системы управления мероприятиями. Тонкий клиент в общем случае - компьютер или программа-клиент в сетях с клиент-серверной архитектурой, который переносит все или большую часть задач по обработке информации на сервер, например компьютер с установленным веб-браузером. В нашем случае - это смартфон с нашим приложением.

Так как вся бизнес-логика сервиса вынесена на сервер, задача приложения по сути представляет из себя отправку запросов и обработку ответов, и последующее отображение данных на смартфоне пользователя. Тонкий клиент является ключевой характеристикой модели SaaS (software as a service), которая используется в системе, вследствие чего для получения прибыли в данном сервисе применяется подход ежемесячной абонентской платы.

Кроссплатформенная разработка

На данный момент существует множество платформ, но доминирующими среди смартфонов являются ОС Android и iOS, которые покрывают более 95% рынка. Соответственно, необходимо разработать как минимум 2 версии приложения, что увеличивает сложность и длительность разработки, тестирования, внедрения и поддержки. Однако в последние годы появились технологии, позволяющие разрабатывать кроссплатформенные мобильные приложения, что значит, что разработанное один раз приложение, можно будет запустить на нескольких платформах без необходимости его переписывать.

Список использованных источников:
1. Microsoft https://visualstudio.microsoft.com/ru/xamarin

ЛИНЕЙНЫЕ СИГНАЛЫ ЦИФРОВЫХ ВОСП

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

Горобец М.С

Тарченко Н.В.

Волоконно-оптическая связь является одним из самых распространенных способов передачи информации в современном мире. За 40 лет своего существования емкость оптических систем связи возросла более чем в 100 000 раз. К настоящему времени емкость коммерческих систем достигла примерно 10 Тбит/с по одному волокну (~100 DWDM-каналов со скоростью 100 Гбит/с в каждом). Основные причины роста трафика: экономическая доступность персональных электронных устройств с камерами и экранами высокого разрешения, развитие сетей широкополосного доступа и подключение к ним все большего количества абонентов, индивидуализация видеоконтента, развитие дата-центров и «интернета вещей». Скоростные сети связи являются технической основой для социальных сетей. Меняется структура самих телекоммуникационных сетей связи, растет скорость клиентских портов.

В связи с ростом объемов передаваемой информации потребность в увеличении скорости передачи информации растет на всех уровнях, начиная с локальных сетей и соединений между компьютерами и заканчивая дальними транспортными сетями, охватывающими всю планету. В настоящее время ведутся разработки когерентных систем с канальной скоростью 400 Гбит/с и 1 Тбит/с и более сложными форматами модуляции (M-QAM). Базовая схема построения когерентного оптического приемника приведена на рисунке 1.

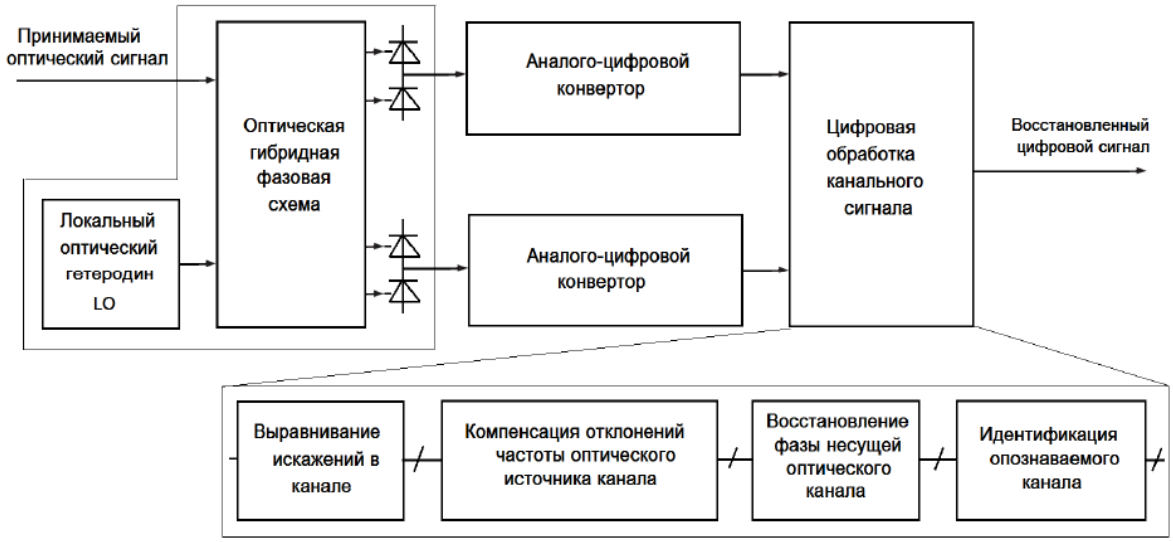


Рис. 1 - Базовая схема построения когерентного оптического приемника с цифровой обработкой сигнала

Увеличение скорости передачи информации сопровождается ростом искажений цифровых сигналов в линии связи. Поэтому растет интерес к форматам модуляции, менее чувствительным к дисперсии и нелинейным искажениям. Они позволяют обеспечить более эффективное использование спектральных каналов в системах плотного волнового мультиплексирования (DWDM) и снизить чувствительность информационных сигналов к искажениям из-за дисперсии или нелинейности.

Таким образом, основными научными и технологическими задачами, над которыми в данный момент активно работают ученые и инженеры в мире, являются:

Совершенствование когерентных систем связи;

Совершенствование методов обработки сигналов в когерентных системах связи;

Совершенствование методов усиления и регенерации оптических сигналов;

Новая инфраструктура волоконно-оптических сетей связи.

Целями данного исследования являются сравнительный анализ методов модуляции в высокоскоростных цифровых ВОСП, а также расчет чувствительности оптического приемника с учетом выбора метода модуляции.

Список использованных источников:
1. Оптическая революция в системах связи и ее социально-экономические последствия – Конышев В.А.
2. Когерентные оптические сети – Фокин В.Г.
3. Новые форматы модуляции в оптических системах связи – Наний О.Е.
4. Тенденции развития оптических систем дальней связи – Леонов А.В.

СЕТЬ ЭЛЕКТРОСВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ МИКРОРАЙОНА С ПОДКЛЮЧЕНИЕМ К ПЛАТФОРМЕ IMS

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

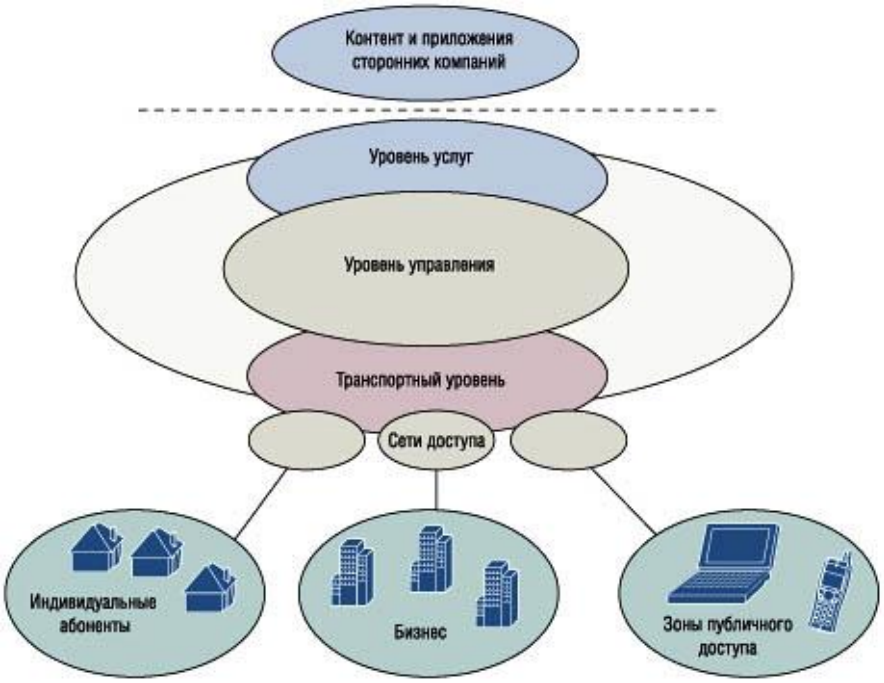
Довнар И.Н.

С развитием инфокоммуникационных систем и сетей, увеличением абонентской базы и появлением необходимости внедрения новых услуг, постоянный поиск технических решений, которые позволят в полной мере удовлетворить спрос на инфокоммуникационные услуги, видится наиболее логичным решением. Так как жизненный цикл систем и сетей телекоммуникаций довольно велик и за этот период происходит значительное количество открытий в науке, возникает желание не обновлять «железо» старых систем, а разрабатывать совершенно новые системы. Таким образом, в начале 21-го века зародилась идея NGN (Next Generation Networks) – сети нового поколения.

Объективными предпосылками к возникновению идеи сетей нового поколения являются:

- успехи пакетных технологий передачи информации, обусловившие бурный рост цифрового трафика, прежде всего за счет расширения использования Интернет;
- увеличение спроса на подвижную связь и на новые мультимедийные службы Triple Play (совместной передачи голоса, видео, данных);
- конвергенция (взаимопроникновение) сетей электросвязи и информационно-вычислительных сетей, развитие инфокоммуникационных сетей.

На базе NGN в последствии была разработана концепция IMS. Ее архитектура представлена ниже на рисунке.



Принцип, на котором строится концепция IMS, состоит в том, что доставка любой услуги никаким образом не соотносится с коммуникационной инфраструктурой (за исключением ограничений по пропускной способности). Воплощением этого принципа является многоуровневый подход, используемый при построении IMS. Он позволяет реализовать независимый от технологии доступа открытый механизм доставки услуг, который дает возможность задействовать в сети приложения сторонних поставщиков услуг.

Список использованных источников:
1. Гольдштейн А.Б., Гольдштейн Б.С. Softswitch. Санкт-Петербург, 2006. – 368 с.

ПОСТРОЕНИЕ ПРИЕМНОГО ТРАКТА С МНОГОПОЗИЦИОННОЙ QAM НА ПЛИС ALTERA

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

Леонович А.В., Ворона В.П.

Тарченко Н.В. – к.т.н.,доцент

Цифровые системы связи уже практически полностью вытеснили своих аналоговых предшественников. Наиболее используемым видом модуляции (если подходить строго, то манипуляции) является квадратурная амплитудная (QAM). Она применяется как в системах с одной несущей, так и в многочастотных, с ортогональным разделением каналов (OFDM), при этом размер сигнального созвездия составляет обычно от 4 до 1024, а в ряде случаев, в частности, в проводных и кабельных системах, встречаются созвездия с размером до 16384[1].

Подсистема состоит из двух идентичных каналов, обеспечивающих формирование комплексной огибающей КАМ-сигнала, представленной квадратурными составляющими I и Q. Последовательность символов забирается с демультиплексора ДМП, являющегося общим для обеих подсистем. Однако в КАМ-подсистеме нечетные разряды подаются в синфазный (I) канал, четные – в квадратурный (Q), или наоборот – правило определяется для конкретного применения[2].

Для формирования *I* и *Q* сигналов используется чтение из ПЗУ предварительно вычисленных отсчетных значений. Такое решение обусловлено необходимостью нормирования амплитуды *I* и *Q* сигналов, чтобы мощность радиосигнала на выходе модулятора была одинаковой для всех режимов.

Ограничение полосы частот выполняет фильтр Найквиста [3]. В зависимости от требований к крутизне склона, неравномерности АЧХ в полосе пропускания, затуханию в полосе задержания и соотношению частоты среза к частоте дискретизации КИХ-фильтр Найквиста будет иметь порядок от 20 и более, т.е. является достаточно ресурсоемким с точки зрения использования блоков ПЛИС (рис. 1).

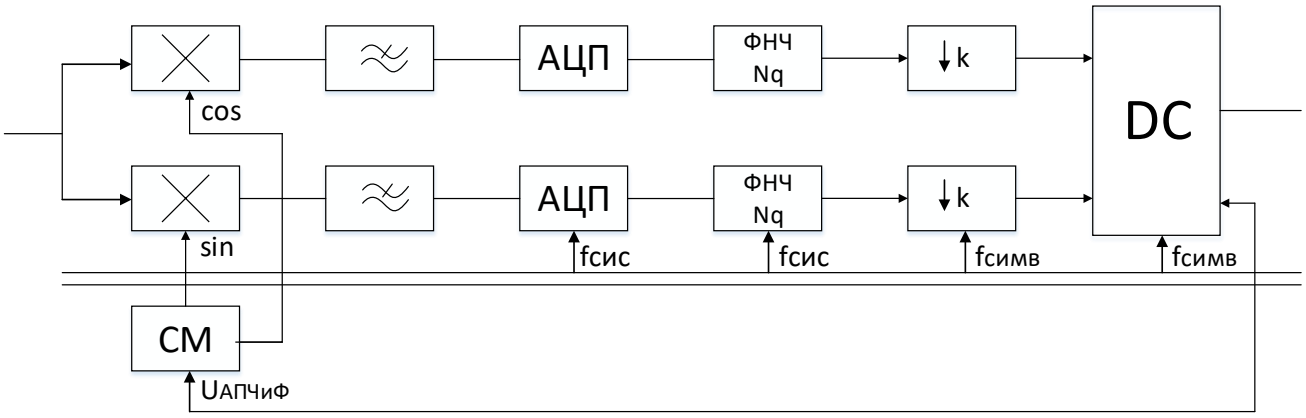


Рисунок 1 – Система формирования QAM сигнала

Сигналы квадратурной амплитудной модуляции M-QAM широко используются при передаче сигналов телевидения по радиорелейным и кабельным линиям, в некоторых системах цифрового телевизионного наземного вещания, передачи сигналов цветности в телевизионном стандарте PAL и NTSC, в стереофоническом радиовещании, в системах программно-определяемого радио (ПОР, SDR).

Список использованных источников:

1. Цифровая обработка сигналов. Сергиенко А. Б. 2002. стр 458,467-468
2. Прокис, Дж. Цифровая связь.: Пер. с англ./под ред. Д.Д. Кловского. – М.: «Радио и связь», 2000. – 800 с.
3. Аналого-цифровое преобразование / под ред. У. Кестера; пер. с англ. под ред. Е.Б.Вологдина. – М.: Техносфера, 2007. – 1016 с.

УМЕНЬШЕНИЕ ФАЗОВЫХ ШУМОВ ГЕНЕРАТОРА ПРИ ВОЗДЕЙСТВИИ ВИБРАЦИИ

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

Ляшук Ю.А., Соколовский Д.В.

Кореневский С.А – к.т.н., доцент

Проведен анализ спектральной плотности фазовых шумов кварцевых генераторов при воздействии вибраций. Разработана, изготовлена и исследована схема электронной компенсации фазовых шумов кварцевых генераторов, позволяющая уменьшить спектральную плотность фазовых шумов кварцевого генератора на 15 – 20 дБ.

Одним из важнейших параметров кварцевого генератора является вибрационная чувствительность, характеризующая уровень увеличение фазовых шумов кварцевого генератора при воздействии вибраций [1, 2]. Анализ справочных данных показывает, что при воздействии на кварцевый генератор вибрационного шумового сигнала, имеющего уровень спектральной плотности 0,04 G^2/Гц, приводит к увеличению спектральной плотности шума кварцевого генератора на 20 – 40 дБ. Применение виброгасителей позволяет уменьшить спектральную плотность фазовых шумов генератора на 15 – 20 дБ, однако в диапазоне низких частот 10 – 200 Гц эффективность виброгасителей значительно уменьшается. Поэтому в работе рассмотрена электронная схема компенсации фазовых шумов кварцевого генератора при воздействии вибраций.

Основой этих схем является формирование на выходе электронной схемы сигнала компенсации, который при подаче на вход частотной модуляции кварцевого генератора сформирует на его выходе спектральные составляющие равные по величине и отличающиеся по фазе на 180 градусов от спектральных составляющих фазовых шумов генератора, обусловленных вибрацией. Для этого целесообразно использовать кварцевые генераторы, имеющие вход коррекции частоты выходного сигнала.

Структурная схема цифровой компенсации фазовых шумов кварцевого генератора приведена на рисунке 1.

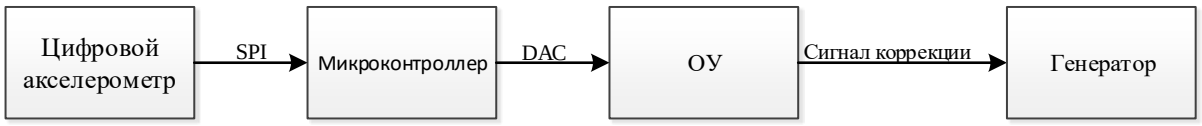


Рисунок 1 – Схема электрическая структурная макета цифровой компенсации фазовых шумов кварцевого генератора

Схема содержит:

- цифровой акселерометр, установленный на кварцевом генераторе, на выходе которого формируется временная зависимость ускорения по трем осям генератора в результате воздействия вибраций;
- микроконтроллер, который обеспечивает установление необходимых значений амплитуд и фаз сигналов по различным осям, суммирование сформированных цифровых сигналов и формирование суммарного аналогового выходного сигнала;
- операционный усилитель обеспечивает требуемое значение выходного напряжения и сопротивления схемы цифровой компенсации.

Сигнал коррекции поступает на вход коррекции частоты кварцевого генератора.

Макет цифровой компенсации имеет следующие параметры:

- чувствительность не менее ±8g;
- наличие встроенного аналогового фильтра;
- частота дискретизации АЦП - 4кГц;
- разрядность АЦП 20 бит;
- интерфейс - SPI;
- тактовая частота микроконтроллера 24 МГц;
- разрядность ЦАП - 12 бит;
- изменение фазы сигналов в каждом канале 0; 180 градусов.

Проведенные результаты экспериментальных исследований показали, что применение разработанной схемы компенсации позволяет уменьшить вибрационную чувствительность кварцевого генератора на 15 – 20 дБ в диапазоне вибрационных частот 20 – 200 Гц.

Список использованных источников:

1. Acceleration "G" Compensated for VCOCXO Based on Digital Controller. QingXiao Shan, Yang Jun, JianYun chen, Tang Qian, LongZhe Ji. Mechatronic and Automation school National University of Defense Technology Changsha, Hunan, China.
2. StevenSteven J. Fry, Gregory A. Burnett, Reducing the acceleration sensitivity of AT-strip quartz crystal oscillators, 2010 IEEE frequency control symposium, page: 25-30.

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ОБРАБОТКИ СИГНАЛОВ С МНОГОПОЗИЦИОННОЙ QAM В СРЕДЕ MATLAB (SIMULINK)

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

Ворона В.П., Леонович А.В.

Тарченко Н.В. – к.т.н.,доцент

QAM (квадратурная амплитудная модуляция) широко используется в качестве схемы модуляции для цифровых телекоммуникационных систем. На сегодняшний день, грамотное применение QAM сопряжено с постоянным моделированием процессов обработки сигналов многопозиционной QAM. Разработанная модель позволяет смоделировать работу системы связи с частотными и фазовыми сдвигами.

Блок Coarse Frequency Compensator позволяет компенсировать частотные искажения, внесенные штатным блоком Phase/Frequency Offset из состава Simulink. Компенсация возможна благодаря грубой подстройке частоты, которая основана на спектральном анализе принятого сигнала. Алгоритм реализован при помощи такого же блока вращения фазы и частоты, при этом на вход блока подается значение частоты на которое необходимо сместить сигнал. Для расчета этой частоты необходимо возвести входной комплексный сигнал в четвертую степень. Таким образом, из сигнала исключается модулированная составляющая и остается только тон частотного сдвига. Тон частотного сдвига можно детектировать при помощи преобразования Фурье.

Блок Carrier Synchronizer представляет из себя контур фазовой автоподстройки частоты. В первую очередь он осуществляет детектирование ошибки фазы, а за тем, после прохождения фильтра, выполняет формирование сигнала компенсации

Для более тщательной проверки алгоритмов синхронизации возможна установка произвольного отношения сигнал/шум в блоке внесения аддитивного белого гауссовского шума. Кроме того, в разработанной модели существует возможность изменять относительную скорость кода в блоке сверточного кодирования. Сверточный код позволяет обнаруживать и исправлять ошибки, возникающие в канале связи. Блок декодера по алгоритму Витерби обеспечивает декодирование входящего сигнала.

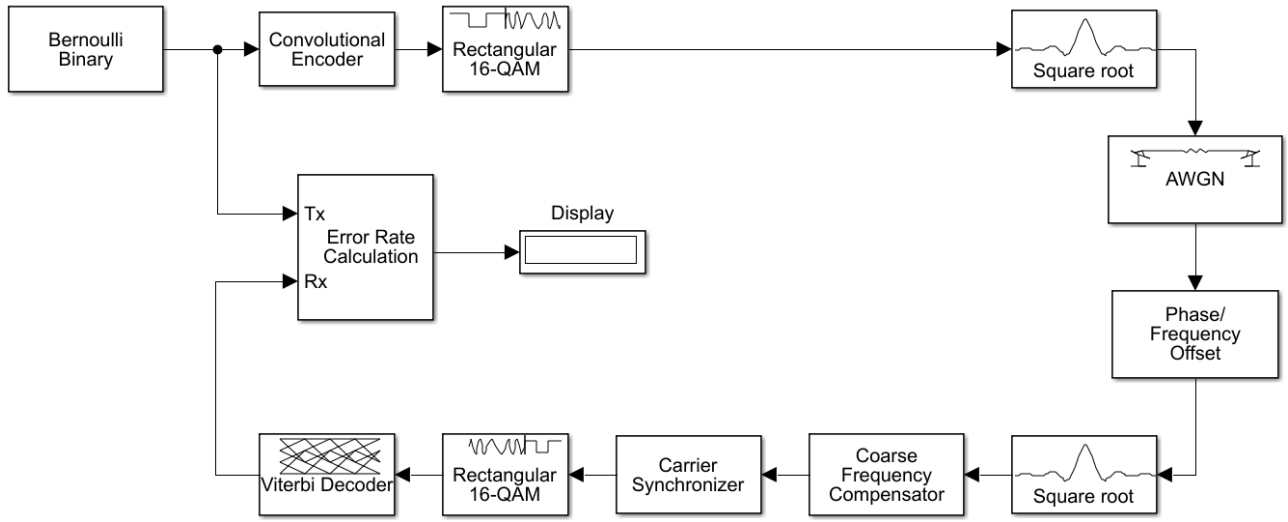


Рисунок 1 – Структурная схема системы связи с частотными и фазовыми сдвигами

Моделирование показало, что полностью разрушенное, с точки зрения фазы, на выходе приемного фильтра сигнальное созвездие, после блока компенсации частотных искажений принимает вид вращающегося созвездия. После контура ФАПЧ система полностью компенсирует все внесенные каналом искажения.

Список использованных источников:

1. Wang, Y., K. Shi, and E. Serpedi. “Non-Data-Aided Feedforward Carrier Frequency Offset Estimators for QAM Constellations: A Nonlinear Least-Squares Approach.” EURASIP Journal on Applied Signal Processing. 2004:13, pp. 1993–2001.

2. Luise, M. and R. Regiannini. “Carrier recovery in all-digital modems for burst-mode transmissions.” IEEE® Transactions on Communications.Vol. 43, No. 2, 3, 4, Feb/Mar/April, 1995, pp. 1169–1178.

УВЕЛИЧЕНИЕ ПРОТЯЖЁННОСТИ УЧАСТКА РЕГЕНЕРАЦИИ ОПТИЧЕСКОЙ ТРАНСПОРТНОЙ СЕТИ

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

Тарченко Н.В.

Волоконно-оптическая система передачи состоит из приёмопередающих модулей, которые в свою очередь состоят из приёмника и передатчика и 2-х оптических волокон (ОВ) (без учёта запаса). Оптический передатчик преобразует электрический сигнал в оптическое излучение с заданными параметрами, которое передаётся по волокну. Оптический приёмник преобразует оптическое излучение в электрический сигнал, выделяет тактовую частоту и передаёт последующим устройствам. Существуют различные способы увеличения пропускной способности волоконно-оптических систем передачи. Применительно к многоканальным ВОСП методы формирования групповых сигналов можно разделить на 2 вида: электронное мультиплексирование и оптическое мультиплексирование. Так же для снижения линейной скорости применяются различные полососберегающие виды модуляции (QAM).

Электронное мультиплексирование часто представляет собой временное разделение каналов. Недостатками такого метода является сложность формирования последовательности бит на больших скоростях и неэффективность передачи трафика по сетям с разделением каналов. Оптическое мультиплексирование приставляет собой спектральное разделение сигналов, то есть каждому сигналу отводится своя полоса пропускания, и эти сигналы независимы друг от друга. Это позволяет реализовать как оптическую кросскомутацию, так и ввод/вывод оптического сигнала определённой длинны волны в промежуточных пунктах.

В волоконно-оптических системах передачи применяются различные способы увеличения протяжённости участка регенерации: улучшение параметров ОВ, применение когерентного приёма, применение оптических усилителей, устройств компенсации дисперсии, цифровой обработки сигналов и предварительная коррекция ошибок. В зависимости от устройств, применяемых при регенерации, различают 3 схемы регенерации: 1R – регенерация мощности имульса, 2R – регенерация мощности и формы импульса, 3R – регенерация мощности, формы и временного положения импульса.

Улучшение параметров ОВ происходило в несколько этапов. Изначально применялись многомодовые ОВ со ступенчатым профилем преломления. Позже были применены ОВ с градиентным профилем преломления. Сейчас используются одномодовые оптические волокна, что позволило устранить межмодовую дисперсию и увеличить скорость передачи. Затухание ОВ во 2-м (1.31 мкм) и 3-м (1,55 мкм) окнах прозрачностисоставляют соответственно 0,375 и 0,275 дБ/км.

Следующим этапом увеличения протяженности участка регенерации стало применение оптических усилителей (ОУ), что позволило увеличить дальность передачи. ВОСП с волокном G.653 на скорости 40 Гбит/с имеют дальность передачи до 1000 км. Применяются 2 типа усилителей: EDFA и Рамановские усилители. EDFA представляет собой волокно, легированное эрбием, его основным недостатком являются неравномерность амплитудно-волновой характеристики и работа только в 3-м окне прозрачности. Романовские усилители представляют собой телекоммуникационное оптическое волокно, в которое вводят оптическое излучение большой мощности, которое вызывает нелинейное вынужденное комбинационное рассеивание для получения распределённого усиления вдоль оптического волокна. Достоинства: большой диапазон усиления, низкий уровень шумов, высокая эффективность.

На более поздних этапах для компенсации хроматической дисперсии стали применяться устройства компенсации дисперсии. На данный момент есть 2 типа устройств компенсации дисперсии: распределённые волоконные компенсаторы, дискретные компенсаторы. 1-е представляют собой волокна с отрицательной по знаку дисперсией и позволяют компенсировать дисперсию с положительным знаком. Из достоинств можно отметить: широкополосность, отсутствие требования температурной стабилизации. Недостатком же является большое затухание. 2-е же основаны на решётках, компенсирующих дисперсию. Достоинства: малый размер и вносимое затухание. Недостатки – узкополосность и значительная температурная зависимость.

Предварительная коррекция ошибок позволяет до десяти дБ увеличить энергетический потенциал участка регенерации, и основана на том, что при передаче вносится избыточность таким образом, чтобы на приёме можно было исправить некоторые типы моделей ошибок. Для этого используются блочные и свёрточные коды. В 1-м случае к каждому информационному блоку ставится в однозначное соответствие кодовое слово. Во 2-м – каждый бит зависит от предыдущего бита (то есть присутствует память). Среди первого типа кодов применяются коды БЧХ и Рида-Соломона, так как они дают достаточно большую эффективность.

Список использованных источников:
1. Бернард Скляр Цифровая связь. Теоретические основы и практическое применение. 2-е издание

СЕМАНТИЧЕСКАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ В ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ

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

Бен Кафо Али Ахмед Саид

Саломатин С. Б.. – к.т.н., доцент

Развитие современных инфокоммуникационных сети, направлено на автоматизацию, интеграцию и повторное использование данных в различных веб-приложениях. Это предъявляет новые требования к механизмам безопасности, особенно в моделях управления доступом. Доступ к ресурсам может контролироваться безопасным способом, если решение о доступе учитывает семантические отношения между объектами в моделями данных сети.

Контроль доступа - это механизм, который позволяет владельцам ресурсов определять, управлять и обеспечивать соблюдение условий доступа, применимых к каждому ресурсу [1-3]. Механизм контроля доступа с учетом семантики должен гарантировать, что только правомочные пользователи имеют право на получение права доступа, и каждый правомочный пользователь должен иметь возможность доступа ко всем ресурсам, на которые он / она авторизован [4].

Традиционные модели управления доступом, такие как MAC, DAC и RBAC, не решают эту проблему, поскольку они не учитывают многообразие семантических отношений в моделях данных.

Семантическая модель управления доступом (SBAC) в процессе принятия решений рассматривает семантические отношения между различными объектами в субъектных, предметных областях и в области действий.

Принятие решений на основе изолированных объектов при игнорировании семантических взаимосвязей между ними может привести к незаконным доступам неавторизованных пользователей и неполному предоставлению прав доступа.

Рассмотрим семантическую модель управления доступом (SBAC), которая аутентифицирует пользователей на основе их учетных данных, предоставляемых в процессе запроса на право доступа.

Положим, что SBAC принимает решения по трем областям: предмет, объект и действие и состоит из трех основных компонентов: базы онтологий, базы авторизации и операций. База онтологий - это набор онтологий: предметная онтология (SO), объектная онтология (OO) и онтология действия(AO).

Объектная онтология. Объекты - это сущности, к которым осуществляется доступ и / или изменения. Объект принадлежит объектной онтологии, которая показывает структуру, в которой объекты (концепции, индивидуумы и свойства) организованы вместе с семантическими отношениями между ними.

Предметная онтология. Субъекты являются активными субъектами требующим доступа к объектам. Субъектами являются понятия или отдельные лица в предметной онтологии. Представление учетных данных определяет право пользователей на доступ к ресурсу.

Антология действия. AO зависbt от типа действий, которые субъекты стремятся выполнить над объектом. Каждый тип действия является концепцией в онтологии, а действия являются индивидуумами концепции, определенной в AO.

Моделируя домены управления доступом с использованием онтологий, SBAC стремится учитывать семантические отношения на разных уровнях онтологии при принятии решения о запросе доступа. При этом используется база авторизации - набор правил авторизации в форме (s, o, ± a), в которых s - это объект в SO, o - это объект, определенный в OO, и a - это действие, определенное в AO. Поскольку SBAC работает на основе логического вывода для предотвращения распространения одного и того же решения (предоставить / запретить) на все выведенные правила, он позволяет определять правила исключения с более высоким приоритетом.

SBAC может быть использована как модель управления доступом для защиты ресурсов SemanticWeb.SBAC учитывает семантические взаимосвязи между объектами в областях принятия решений по управлению доступом. Автоматическое принятие решений в SBAC о предоставлении или отклонении запроса на доступ осуществляется через процессы логического вывода на основе семантического отношения между объектами.

Список использованных источников:

1. Hengartner, U., Steenkiste, P.: Exploiting information relationships for access control. In: proceeding of third IEEE International Conference on Pervasive Computing and Communications, Percom 2005, Kauai, Island HI (2005) 278–296
2. Bonatti, P.A., Duma, C., Fuchs, N., Nejdi, W., Olmedila, D., Peer, J., Shahmehri, N.: Semantic web policies – a discussion of requirements and research issues. In:ESWC 2006. (2006) 712–724
3. Samarati, P., di Vimecati, S.C.: Access control: Policies, models, architectures. In:FOSAD 2000. Volume 2171 of LNCS., Springer-Verlag (2001) 137–196
4. Qin, L., Atluri, V.: Concept-level access control for the semantic web. In: ACM Workshop on XML Security, Fairfax, VA, USA (2003) 94–103

НЕОПРЕДЕЛЕННОСТЬ ИЗМЕРЕНИЯ ДИЭЛЕКТРИЧЕСКОЙ ПРОНИЦАЕМОСТИ

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

Певнева Н.А.

На основании априорной информации (параметров, характеризующих волноводную измерительную систему, и результатов измерений) можно оценить неопределенности результатов измерений, проведенных с помощью метода диэлектрического стерженька и модифицированного метода свободного пространства

Диэлектрическая проницаемость материалов определялась по методам, описанным в [1] – [3].

В таблице 1 приведены рассчитанные составляющие неопределенности диэлектрической проницаемости трансформаторного масла на частоте 10 ГГц (ε = 2,43). В таблице 2 приведены рассчитанные составляющие неопределенности диэлектрической проницаемости текстолита на частоте 34 ГГц (ε = 3,3). В таблице 3 приведены рассчитанные составляющие неопределенности диэлектрической проницаемости оксида меди на частоте 100 ГГц (ε = 1,55).

Таблица 1 – Результаты расчета неопределенности

u(S1)	u(S2)	u(f)	u(a)	u(ΔX)	u(d)	u(λ0)	u(A)
0,7402	0,1732	0,0000058	0,0000289	0,000289	0,0000289	-1,7·10-11	0,0000868
u(B)	u(G)	u(D)	u(β)	u(γ)	u(ε')	u(ε")	u(ε)
0,05115	-0,4712	0,000536	13,98	14,93	0,035583	0,037068	0,051383
Для трансформаторного масла на частоте 10 ГГц расширенная неопределенность составила 0,103, что в процентном соотношении соответствует 4,2 %.							

Таблица 2 – Результаты расчета неопределенности

u(|So|)	u(|Sи|)	u(φo)	u(φи)	u(f)	u(a)	u(l)	u(d)
0,23094	0,18937	2,887	2,887	0,0000058	0,0000289	0,0000289	0,0000289
u(λ0)	u(no)	u(nи)	u(αo)	u(αи)	u(B)	u(G)	u(A)
-1,5·10-12	-0,26588	-0,21698	1,555	1,555	6,95	1,58	0,0000217
u(D)	u(β)	u(γ)	u(ε')	u(ε")	u(ε)		
0,0000114	30,24	23,33	0,0215	0,0270	0,0345		
Для текстолита на частоте 34 ГГц расширенная неопределенность составила 0,069, что в процентном соотношении соответствует 2,1 %.							

Таблица 3 – Результаты расчета неопределенности

u(|S11|)	u(|S21|)	u(φ11)	u(φ21)	u(f)	u(d)	u(λ0)	u(Г)
0,1622	-0,1155	4,619	3,464	577,35	0,0289	-0,0052	5,26
u(K)	u(T)	u(Λ)	u(S11)	u(S21)	u(ε)		
3,75	17,46	0,112	2,99	2,39	0,0195		
Для оксида меди на частоте 100 ГГц расширенная неопределенность составила 0,039, что в процентном соотношении соответствует 2,5 %.							

Результаты оценки показали, что исследования по методу диэлектрического стерженька с использованием САЦ обеспечивают неопределенность результатов ±5 % при доверительной вероятности Рд = 0,95. Исследования по методу диэлектрического стерженька с использованием ВАЦ обеспечивают неопределенность результатов ±2,5 % при доверительной вероятности Рд = 0,95. Исследования по модифицированному методу свободного пространства обеспечивают неопределенность результатов ±3 % при доверительной вероятности Рд = 0,95.

Список использованных источников:

1. Певнева, Н. А. СВЧ метод определения диэлектрических свойств жидкостей / Н. А. Певнева, А. В. Гусинский, А. Л. Гурский // Доклады БГУИР. – 2012. – № 5 (67). – С. 46–50.

2. Певнева, Н. А. Использование метода цилиндрического стерженька и векторного анализатора цепей для определения диэлектрической проницаемости материалов в СВЧ диапазоне / Н. А. Певнева, А. Л. Гурский, А. М. Кострикин // Доклады БГУИР. – 2019. – № 1 (119). – С. 56–61.

3. Певнева, Н. А. Метод свободного пространства с использованием векторного анализатора цепей для определения диэлектрической проницаемости материалов на СВЧ / Н. А. Певнева, А. Л. Гурский, А. М. Кострикин // Доклады БГУИР. – 2019. – № 4 (122). – С. 32–39.

ПРИМЕНЕНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ МУЛЬТИРОТОРНОГО ТИПА В ИНТЕРЕСАХ ВООРУЖЕННЫХ СИЛ

Алексеенко А.Э., Чепикова В.В.

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

Цветков В.Ю – д.т.н., доцент

Применение беспилотных летательных аппаратов мультироторного типа значительно расширяет возможности военнослужащих пограничных войск. В работе проведен краткий обзор возможной комплектации беспилотных летательных аппаратов мультироторного типа, а также сделаны выводы о целесообразности их использования при охране государственной границы.

Создание и применение в мире беспилотных летательных аппаратов (БЛА) стало серьезным прорывом в области интеллектуальных достижений. Инновации использованы во всех элементах этих устройств: от современных композитных материалов до новейшего охранного оборудования. БЛА мультироторного типа представляет собой радиоуправляемую летающую платформу с 3, 4, 6, 8, 12 бесколлекторными двигателями с пропеллерами. В полете платформа занимает горизонтальное положение относительно поверхности земли, может зависать над определенным местом, перемещаться влево, вправо, вперед, назад, вверх и вниз, а также поворачиваться вокруг своей оси.

БЛА мультироторного типа имеет ряд преимуществ:

– имеет возможности зависать над объектом, находясь в непосредственной близости от чрезвычайной ситуации;

– делать фронтальные снимки объектов для создания более точных 3D моделей;

– возможность вертикального взлета для задач с ограниченной взлетно-посадочной площадью.

Применение БЛА для защиты государственных границ является востребованным и эффективным. БЛА мультироторного типа могут оснащаться системами распознавания лиц и номерных знаков автомобилей, тепловизорами, технологией перехвата телефонных звонков. Это очень удобно для предотвращения и реагирования на инциденты на границе. К тому же, это позволяет контролировать ситуации в малодоступных приграничных районах. Важным является тот факт, что аппараты будут использоваться для дневных и ночных операций.

Для усовершенствования работы военнослужащих пограничных войск с применением БЛА мультиротерного типа предлагается оснастить устройства дополнительно проблесковыми маячками синего и красного цвета, как у техники специального назначения, двумя громкоговорителями и ярким светодиодным прожектором. Кроме того, на аппарате должны быть установлены видеокамера и камера ночного видения, а также тепловизор. Важно дополнительно оснастить БЛА мультироторного типа системой автоматической подзарядки. Таким образом, во время патрулирования при снижении заряда аккумулятора до нескольких процентов, аппарат будет иметь возможность вернуться на ближайшие месторасположение зарядных устройств БЛА мультироторного типа и самостоятельно подключиться к зарядному устройству. С помощью специального пульта управления оператор сможет задать план патрулирования территории и передать его на рабочее место дежурного. Это позволит БЛА мультироторного типа вести охрану в автономном режиме. Важно отметить, что для постоянного контроля за территорией необходимо иметь несколько БЛА мультироторного типа, которые будут покрывать одну и ту же территорию, т.е. будут замещать друг друга.

При обнаружении нарушителя с помощью БЛА мультироторного типа оператор будет иметь возможность отправить сигнал тревоги и начнет запись видеотрансляции. Одновременно с этим оператор сможет включить вспышки проблесковых маячков на устройстве для обозначения места нахождения нарушителей для ситуаций, в которых отряд быстрого реагирования находится на близком расстоянии. Также БЛА начнет проигрывать через громкоговорители заранее записанные предупреждающие фразы.

Необходимо также принять во внимание тот факт, что нарушители государственной границы могут быть вооружены, т.е. у них будет возможность сбить или уничтожить БЛА. Поэтому важно с заданным периодом времени отправлять на пульт оператора данные о местонахождении аппарата, чтобы в случае потери связи с ним другой БЛА мог начать патрулирование сразу с заданных координат, а не по установленному маршруту.

Таким образом, с использованием БЛА мультироторного типа усовершенствованной комплектации, военнослужащие пограничный войск могут отслеживать нарушителей и препятствовать незаконному пересечению границы в труднопроходимых зонах.

SHAREPOINT 2016 ODATA УЯЗВИМОСТЬ

Трафимук М.П.

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

Селезнев И.Л. – к.т.н.,доцент

В современном мире все большее количество услуг и сервисов предоставляется посредством сети Интернет, поскольку Интернет и, соответственно, все его ресурсы доступны повсеместно. Помимо описанных положительных сторон есть и отрицательные: доступность, стабильность и надежность зависят не от пользователя, а от владельца ресурса. Обеспечить максимальную стабильность – это первостепенная задача администратора ресурса, для выполнения которой необходимо знать возможные уязвимости и способы их устранения.

С течением времени все большее количество услуг и сервисов предоставляется посредством сети Интернет. Повсеместное распространение доступа к сети и ее ресурсам является основной причиной этого явления. Помимо положительных сторон этого явления есть и отрицательные моменты: доступность, стабильность и надежность зависят не от пользователя, а от владельца ресурса. Обеспечить максимальную стабильность – это первостепенная задача администратора ресурса, для выполнения которой необходимо знать возможные уязвимости и способы их устранения.

На сегодняшний день ключевые ресурсы сети Интернет являются достаточно устойчивыми к различного вида атакам, использующим уязвимости протоколов UDP и TCP, а также DNS-серверов и других широко используемых сущностей. Ранее использование недоработок в этих компонентах для реализации атак приводило к неприятным последствиям для владельцев и администраторов ресурсов сети Интернет. Ключевой идеей этих, устаревших на данный момент, атак является генерация и отправка больших потоков данных атакуемому ресурсу.

Многие люди используют инструменты, предоставляемые Google для создания и редактирования документов, так как эти ресурсы бесплатны и доступны, однако они не удовлетворяют требованиям безопасности и функциональности для средних и крупных компаний. Такие компании, как правило, используют платную продукцию других компаний, среди которых наиболее широко известна компания Microsoft. Корневым узлом в инфраструктуре инструментария Microsoft со схожим, но более широким функционалом является Microsoft SharePoint Server. Он используется во многих серверах на базе Microsoft IIS, которых на данный момент 41,5% в сети Интернет [1]. Соответственно, уязвимость в корневом узле является блокирующей уязвимостью для всех поддерживаемых сервисов.

В Microsoft SharePoint Server 2016, самом актуальном на сегодняшний день, существует уязвимость, унаследованная от библиотеки Microsoft.Data.OData, которая обрабатывает и разбирает входящие запросы на составляющие части, после чего передает обработанную версию далее для верификации и исполнения. Уязвимость заключается в том, что при использовании фильтра некоторые комбинации вызывают критическую ошибку при обработке запроса, вследствие чего процесс останавливается и в автоматическом режиме запускается снова. Однако в качестве защиты от дестабилизации сервера перезапуск процесса происходит только 10 раз. По истечении 10 перезапусков восстановить работу можно только при ручной обработке ошибки и перезагрузке всей системы.

Алгоритм атаки следующий:

1) Установить подключение по SSL,
2) Проверить доступность сервера,
3) Сформировать вредоносный пакет, ключевым элементом которого является строка “filter=true”+”+or+true”*N, где N>=6100,
4) Отправить пакет серверу,
5) Перейти к пункту 1.

Таким образом, используя всего один компьютер, можно сделать недоступным Microsoft SharePoint Server 2016 приблизительно за 5 минут; этого времени, как правило, достаточно для автоматического перезапуска процесса и подготовки к приему новых пакетов для всех 10 итераций, необходимых для приведения сервера в недоступное состояние. Ключевой и единственной проблемой реализации данной атаки является необходимость установки подключения по SSL, что, в свою очередь, требует наличия корректного логина и пароля. В результате атаки для внешнего наблюдателя сервер на любой HTTP запрос будет отправлять код ответа из 500 серии, как правило, код 503 или, в редких случаях, 500. На момент написания данной статьи эта уязвимость не имеет способов устранения, однако известна компании Microsoft под кодом CVE-2018-8269.

Список использованных источников:

5. December 2018 Web Server Survey [Электронный ресурс]. – Режим доступа: https://news.netcraft.com/archives/2018/12/17/

О ДЕКОДИРОВАНИИ НЕКОТОРЫХ ВИДОВ ОШИБОК В ДВУМЕРНЫХ КОДАХ-ПРОИЗВЕДЕНИЯХ

Липницкий В.А., Сергей А.И.

Военная академия Республики Беларусь
Гродненский государственный университет имени Янки Купалы

В статье описывается подход к решению задачи точного декодирования двумерных кодов-произведений, построенных на основе двоичных линейных кодов. Формулируется и доказывается лемма, которая служит вспомогательным инструментом для построения алгоритма исправления любых конфигураций ошибок в пределах теоретической корректирующей способности кода-произведения.

Идея кодов-произведений заключается в построении мощных помехоустойчивых кодов на основе более простых базовых кодов.

Кодом-произведением $C = C_1 \times C_2$ называется код, словами которого являются все двумерные матрицы со строками, являющимися словами кода C_1 и столбцами, являющимися словами кода C_2. При этом минимальное расстояние кода C равно произведению минимальных расстояний кодов сомножителей [1]. Способ построения кодов-произведений с высокими корректирующими возможностями описан в [2].

Одним из главных преимуществ кодов-произведений является способность справляться с ситуациями, когда ошибки возникают с высокой частотой в коротком промежутке, т. е. исправлять так называемые пакетные ошибки, нередко встречающиеся на практике. В таких случаях количество реально исправленных ошибок сильно превосходит теоретическую корректирующую способность кода.

Для практических применений скорость часто оказывается более важным параметром, чем качество декодирования, поэтому широкое распространение получили так называемые блочные турбокоды. Для расшифровки турбокодов применяют, как правило, простую итеративную процедуру, которая представляет собой компромисс между скорость работы и качеством дешифровки. Существуют конфигурации ошибок, которые итерационный метод не способен исправить, хотя корректирующая способность кода позволяет это сделать.

Что касается точного декодирования, то существуют подходы, требующие использования базовых кодов специального вида. Например, в [1] описана схема точного исправления ошибок в кодах-произведениях, построенных на основе БЧХ-кодов.

В данной статье исследуется возможность точного декодирования кодов-произведений, сконструированных на основе более широкого класса кодов, а именно двоичных линейных кодов.

Рассмотрим сначала пример построения двумерного кода-произведения. В качестве базовых кодов C_1 и C_2 возьмем классический код Хэмминга (7, 4, 3), исправляющий однократную ошибку. Т. е. в рассматриваемом случае используется один и тот же код и для строк, и для столбцов.

Таким образом, получившийся код-произведение имеет 16 информационных разрядов. Перед началом кодирования биты передаваемого сообщения записываются в виде матрицы 4×4. Далее строки этой матрицы независимо кодируются с помощью базового кода C_1, после чего к столбцам полученной 4×7 матрицы применяется аналогичная процедура, т. е. каждый столбец кодируется с использованием базового кода C_2. В результате получится матрица 7×7, которая и будет кодовым словом, соответствующим передаваемому сообщению.

Можно доказать, что построенный код имеет минимальное расстояние, равное 9, т. е. исправляет четырехкратные ошибки [3].

В общем случае, разумеется, базовые коды для строк и столбцов могут быть различными. Например, если взять за основу коды с параметрами (17, 9, 5) и (15, 11, 3), то полученный в результате код-произведение будет иметь параметры (15×17, 11×9, 3×5) или (255, 99, 15), т. е. позволит исправлять семикратные ошибки [2].

Хотя минимальное расстояние кода-произведения теоретически вычисляется легко, процесс декодирования представляет собой сложную задачу. Вызвано это в первую очередь богатым разнообразием конфигураций возникающих ошибок [4]. Алгоритм декодирования также должен учитывать, что базовые коды могут неверно декодировать или вовсе не обнаружить ошибку в соответствующей строке/столбце, т. к. количество ошибок в отдельно взятой строке/столбце может превышать декодирующую способность базового кода.

Итеративные процедуры декодирования, обычно применяемые для исправления ошибок в кодах-произведениях, многократно повторяют операции поочередного исправлениях ошибок во всех строках, потом во всех столбцах и т. д. При этом, например, при декодировании строк никак не учитывается информация, известная об ошибках в столбцах, необходимая для того, чтобы результаты декодирования по строкам и по столбцам были согласованы друг с другом.

Далее приведена лемма, позволяющая учитывать информацию об ошибках в столбцах при декодировании строк и наоборот.

Лемма 1. Пусть C - линейный код с параметрами [n, k, d]. Для него справедливо следующее свойство:

Пусть известно, что ошибки могли возникнуть только в $s \le d$ заранее известных позициях $i_1, i_2, ..., i_s$ принятого вектора-слова длины n. Рассмотрим бинарный вектор v длины n, в котором в позициях $i_1, i_2, ..., i_s$ стоят единицы, а остальные элементы нулевые.

Если $v \notin C$, тогда синдромы всех возможных 2^s ошибок различны, т. е. можно однозначно исправить любые ошибки веса $\le s$.

Если $v \in C$ (и, следовательно, $s = d$), тогда имеется 2^{d-1} различных синдромов ошибок. Каждый синдром встречается ровно 2 раза: синдром вектора ошибок e совпадает с синдромом вектора $e + v$. Другими словами, вектор ошибок в таком случае определяется с точностью до инвертирования позиций $i_1, i_2, ..., i_d$.

Доказательство.

Пусть H – проверочная матрица кода C.

1. $s \le d - 1$. В этом случае утверждение Леммы 1 напрямую следует из того, что любые $d-1$ матрицы H линейно независимы [1] и образуют базис.

2. $s = d$ и $v \notin C$. Поскольку в матрице H любые $d-1$ столбцов линейно независимы, то столбцы $i_1, i_2, ..., i_d$ могут быть линейно зависимыми только в случае, если $Hv^T = 0$. Но это невозможно, т. к. $v \notin C \Rightarrow Hv^T \neq 0$. Поэтому столбцы $i_1, i_2, ..., i_d$ линейно независимы и все 2^d синдромов различны.

3. $s = d$ и $v \in C$. Пусть A – матрица, образованная столбцами $i_1, i_2, ..., i_d$ матрицы H.

Рассмотрим следующую систему уравнений над $GF(2)$: $Ax^T = y$, где y – произвольный синдром ошибки.

Ранг матрицы A равен $d-1$, поэтому имеется $d-1$ базисных переменных и одна свободная. Таким образом, система имеет ровно два решения. При этом, поскольку $v \in C \Rightarrow Hv^T = 0 \Rightarrow A(1 \ 1 \ \dots \ 1)^T = 0$, значит, если $Ax^T = 0$, то и $A(x + (1 \ 1 \ \dots \ 1))^T = 0$, т. е. кодовое слово определяется с точностью до инвертирования позиций $i_1, i_2, ..., i_d$.

Лемма доказана.

Продемонстрируем возможности применения леммы 1 на примере вышеупомянутого кода [255, 99, 15] ([15 x 17, 11 x 9, 3 x 5]). Этот код позволяет исправить вплоть до 7-ми произвольных ошибок. Заметим, что если ошибки возникли не более чем в 5 столбцах, и при этом в каждом из этих столбцов ошибка была зарегистрирована, то с помощью Леммы 1 можно точно декодировать исходное сообщение по строкам, даже если количество ошибок в отдельно взятой строке выходит за пределы декодирующей возможности кода C_1.

Нетрудно видеть, что существуют конфигурации ошибок, в которых одного только применения Леммы 1 недостаточно для декодирования сообщения. Разбор таких частных случаев является необходимым условием для построения алгоритма точного декодирования кодов-произведений, но выходит за рамки данной статьи.

Такими случаями являются:

- сильно разреженные ошибки, возникающие сразу во многих строках и многих столбцах;
- существование строки/столбца, вектор ошибок в котором представляет собой кодовое слово, а, следовательно, ошибка в этой строке/столбце не будет зарегистрирована.

В статье рассмотрена Лемма 1 – вспомогательный инструмент, которым можно пользоваться при расшифровке кодов-произведений. Использование леммы вместе с разбором нескольких частных случаев позволяет построить алгоритм точного декодирования кодов-произведений [63, 12, 9] ([7 x 9, 4 x 3, 3 x 3]) и [255, 99, 15] ([15 x 17, 11 x 9, 3 x 5]).

Список использованных источников:

6. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. – М. : Мир, 1986. – 576 с.

7. Липницкий В.А. Тензорные произведения кодов Хэмминга. – 11-я Белорусская математическая конференция: Тезисы докладов Междунар. науч. Конф. Минск, 5 – 9 ноября 2012 г. – Часть 4. – Мн.: Институт математики НАН Беларуси, 2012. – С. 62 – 63.

8. Мак-Вильямс, Ф. Дж. Теория кодов исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М. : Связь, 1979. – 744 с.

9. Липницкий В.А., Сергей А.И., Спичекова Н.В. Классификация точечных образов. История и современность. // XI-я Белорусско-российская НТК «Технические средства защиты информации», г. Минск, 5 – 6 июня 2013 г. Тезисы докладов. – Мн.: БГУИР, 2013. – С. 42.

РАЗЛОЖЕНИЕ ФУНКЦИЙ В БАЗИСЕ ПОЛИНОМОВ ЭРМИТА

Раткевич А.С.

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

Власова Г.А. – к.т.н., доцент кафедры защиты информации

Данная работа включает в себя исследование полиномов Эрмита и их свойств, а также примеры разложения нескольких математических функций в базисе данных полиномов.

Чтобы изучить свойства ортогональных полиномов и математических функций, их визуализации (рисунок 1), а также исследовать разложения некоторых математических функций в базисе данных полиномов мною была создана программа на языке JavaScript.

Мною были рассмотрены полиномы Эрмита:

$$H_n^{\text{phys}}(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2}$$

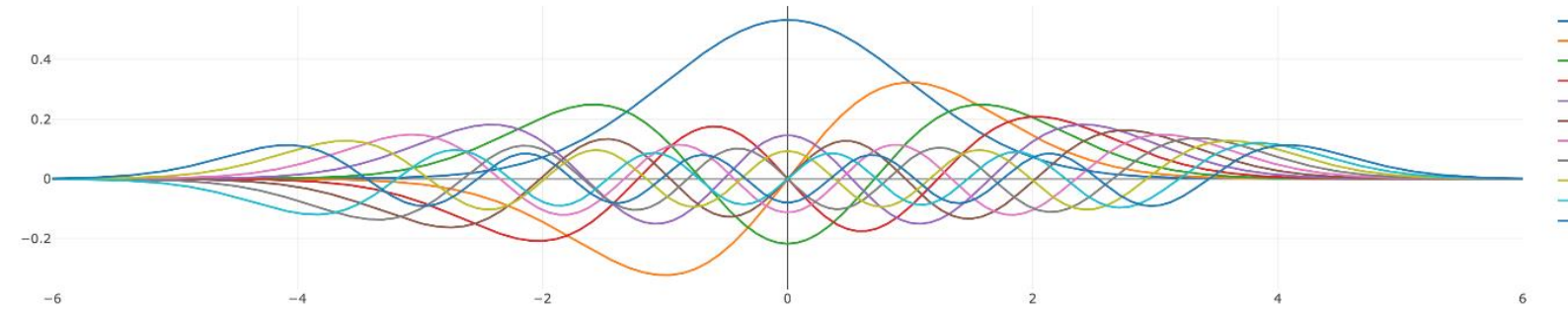


Рисунок 1 – Визуализация на примере полинома Эрмита.

Визуализация и разложение функции cos(3x) в базисе полинома Эрмита приведены на рисунках 2, 3.

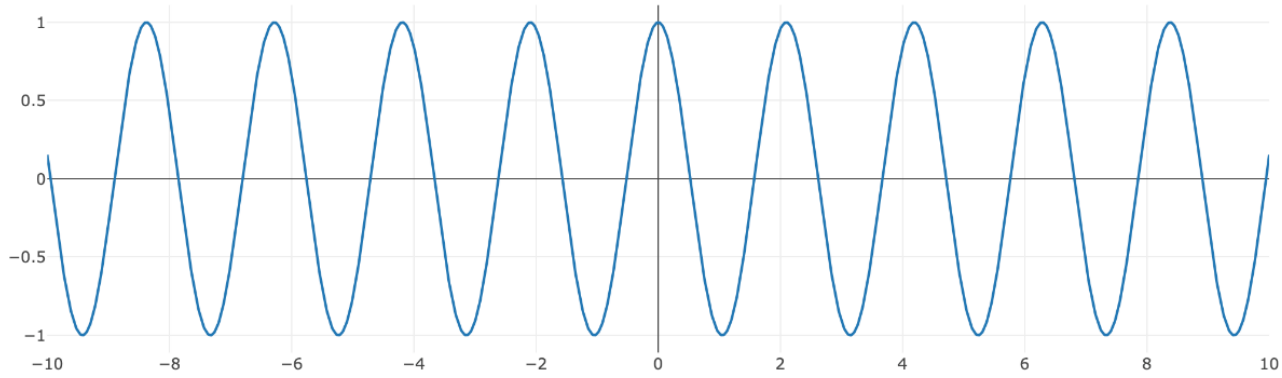


Рисунок 2 – Функция cos(3x)

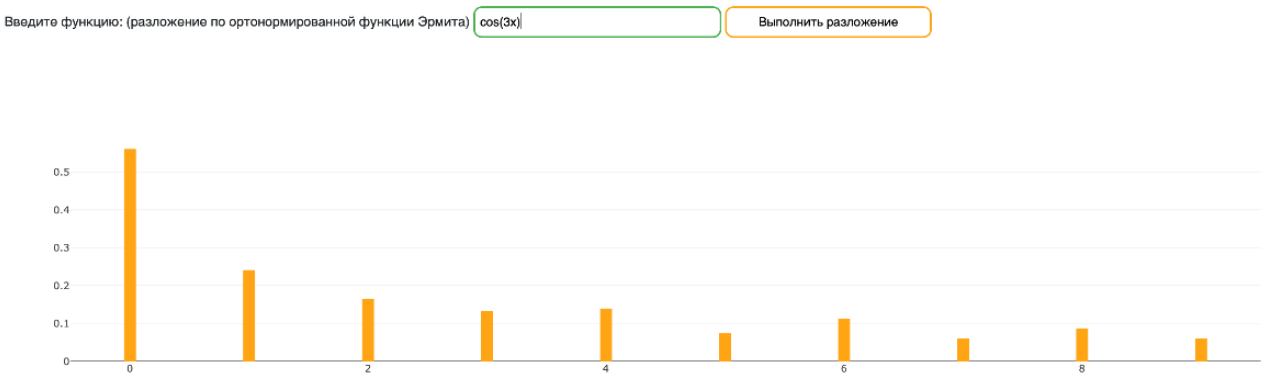


Рисунок 3 – Разложение функции cos(3x) в базисе полинома Эрмита.

Программа предоставляет возможность разложения различных математических функций, например, sin(x)/x, и функции sin(10x)/(10x) (рисунок 4,5).

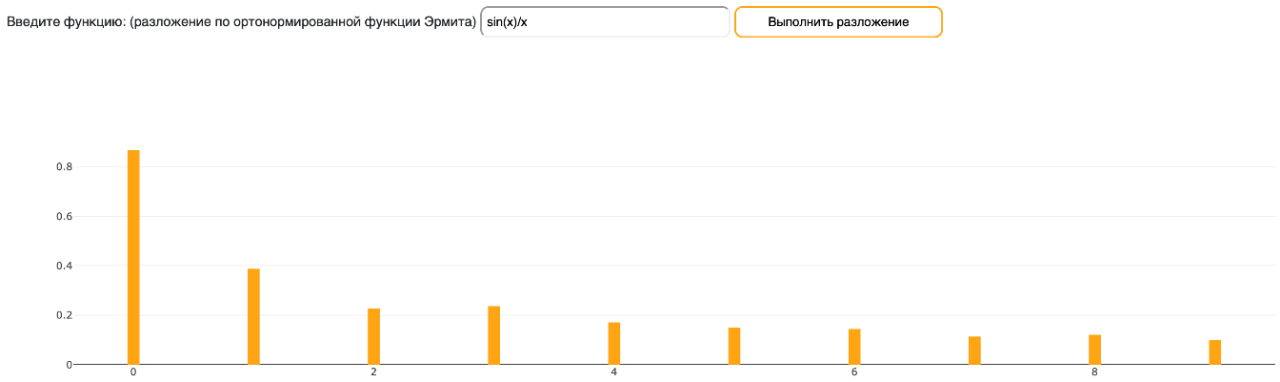


Рисунок 4 – Разложение функции sin(x)/x в базисе полинома Эрмита.

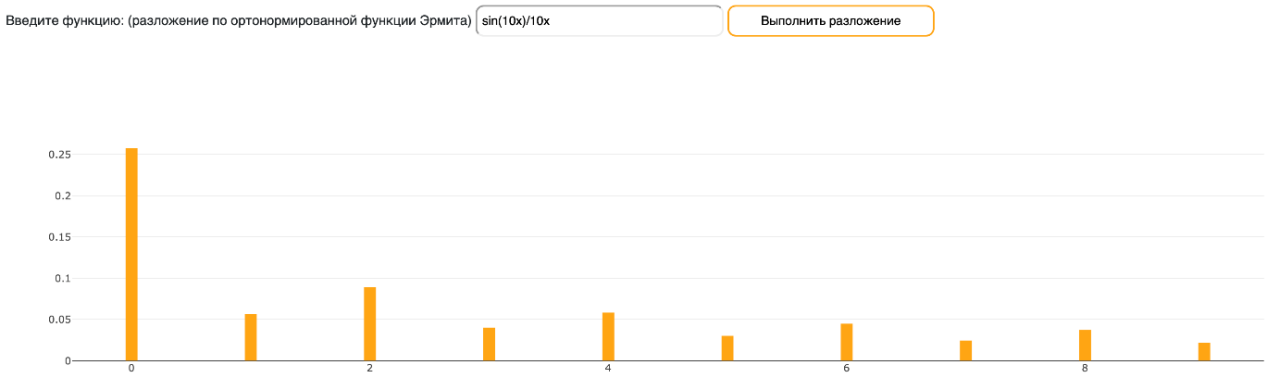


Рисунок 5 – Разложение функции sin(10x)/10x в базисе полинома Эрмита.

Сравнение двух спектров рассмотренных функций показывает, что при увеличении аргумента функции происходит уменьшение значений составляющих, а также увеличение разности значений соседних составляющих.

Список использованных источников:

10. И.С. Гоноровский: Радиотехнические цепи и сигналы. – М.: Радио и связь, 1986 г. – 512 с.

11. Hermite Polynomials [Электронный ресурс]. – Электронные данные. – Режим доступа: http://dsp-book.narod.ru/HFTSP/8579ch22.pdf

ПРОГРАММНОЕ СРЕДСТВО КЛАССИФИКАЦИИ РЕЧИ НА ОСНОВЕ КЕПСТРАЛЬНОГО АНАЛИЗА

Райкевич А.С., Никитенко Ю.Н, Зельманский О.Б.

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

Зельманский О.Б. – к.т.н.,доцент

Предложено программное средство классификации фонетических единиц на фонемы, реализующее заключающийся в нахождении минимума расстояния между кепстрами анализируемой фонетической единицы и базы образцов алгоритм. Данное программное средство позволяет определить к какой группе фонем относится анализируемая фонетическая единица и, кроме того, какой фонеме она соответствует в большей степени.

Устная речь, производимая речевым аппаратом и передаваемая в естественных условиях посредством звуковых волн, сегодня является самым оперативным и распространенным способом передачи информации в любой сфере человеческой деятельности. Поэтому в современных компьютерных системах приветствуется, а в некоторых случаях и является крайне необходимым использование средств речевого взаимодействия с пользователем.

На этапе цифровой обработки сигнала непрерывный электрический сигнал проходит оцифровку и преобразуется в набор параметров. Основной задачей на этом этапе является получение компактных, но в то же время достаточно полно описывающих речевой сигнал характеристик, позволяющих максимизировать показатели эффективности распознавания. Для того чтобы получить векторы признаков одинаковой длины, происходит сегментация речевого сигнала на равные части, а затем выполнение преобразования внутри каждого сегмента. На выходе получается последовательность признаков речевого сигнала.

Для выполнения задачи распознавания речи наиболее эффективными являются кепстральные признаки [1-3]. Кепстральный вектор может быть получен с помощью обратного дискретного преобразования Фурье от логарифма амплитуды спектра, полученного с помощью прямого дискретного преобразования Фурье [1]. Кепстральный анализ применяется для отделения сигнала возбуждения от сигнала речевого тракта. Полученные в таком случае параметры обеспечивают качественное выполнение разделимости звуков – классификацию речи.

В качестве входных параметров программного средства классификации речи используются фонетические единицы речи. Каждая фонетическая единица представляет собой звуковой файл средней длительностью от 30 до 200 мс, записанный в формате WAV. Частота дискретизации для каждого файла 44100 Гц, амплитуда каждого отсчёта характеризуется 32-мя битами.

Блок вычисления кепстральных коэффициентов сигнала выполняет расчет кепстра анализируемого сигнала, который передается в блок вычисления коэффициента различия, на второй вход которого из базы данных звуковых волн аллофонов, содержащей образцы вариантов реализации фонем, обусловленные конкретным фонетическим окружением этих фонем, последовательно поступают значения их кепстральных коэффициентов. В свою очередь блок вычисления коэффициента различия на основе корреляционной матрицы осуществляет расчет коэффициентов различия для анализируемой фонетической единицы и всех образцов, содержащихся в базе данных аллофонов, а также сопоставляет их длительности, результаты вычислений передаются в блок принятия решения. В функции последнего входит принятие решения о принадлежности анализируемой фонетической единицы к той или иной группе фонем, а также ее классификация как определенной фонемы путем нахождения образца с наиболее близкой анализируемой фонетической единице длительностью, которому соответствует наименьшее значение коэффициента различия. Классифицированная фонетическая единица сохраняется в новой базе данных аллофонов или обновляет уже существующую базу.

Таким образом, в ходе работы программного средства формируется массив фонетических единиц, разделенных по классам, которые сохраняются в базе данных звуковых волн аллофонов.

Список использованных источников:

1. Рабинер, Л.Р. Цифровая обработка речевых сигналов: пер. с англ. / Л.Р. Рабинер, Р.В. Шафер; под ред. М.В. Назарова и Ю.Н. Прохорова. – Москва: Радио и связь, 1981. – 495 с.

2. Шарий, Т.В. О проблеме параметризации речевого сигнала в современных системах распознавания речи / Т.В. Шарий // Вісник Донецького національного університету. Сер. А: Природничі науки. 2008. – № 2 [Электронный ресурс] / Національна бібліотека України ім. В.І. Вернадського. – Київ, 2008. – Режим доступа: http://www.nbuv.gov.ua/portal/Natural/VDU/a/2008_2/Control%20systems/9_Shariy.pdf. – Дата доступа: 1.11.2010.

3. Граничин, О.Н. Решение задачи автоматического распознавания отдельных слов речи при помощи рандомизированного алгоритма стохастической аппроксимации / О.Н. Граничин, Д.С. Шалымов // Нейрокомпьютеры: разработка, применение. – 2009. – № 3. – С. 58–64.

КОНЦЕПЦИЯ АДАПТИВНОГО УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

Полещук В.С., Ширинский В.П., Некрашевич И.Г.

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

Ширинский В.П. – к.т.н.,доцент

В работе приводится описание модели адаптивной безопасности сети. Дано обоснование подхода к адаптивному управлению безопасностью информационных систем. Приведены основные классификационные признаки объектов управления в концепции адаптивного управления.

Непрерывное развитие сетевых технологий при отсутствии постоянно проводимого анализа их безопасности и нехватки ресурсов для обеспечения защиты приводит к тому, что с течением времени защищенность корпоративных инфологических систем падает, так как появляются новые неучтенные угрозы и уязвимости системы.

Адаптивный подход к безопасности позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на риски безопасности, используя правильно спроектированные и хорошо управляемые процессы и средства.

Адаптивная безопасность сети состоит их трех основных элементов:

- технологии анализа защищенности;
- технологии обнаружения атак;
- технологии управления рисками.

Анализ защищенности – это поиск уязвимых мест в сети. Сеть состоит из соединений, узлов, рабочих станций, приложений и баз данных. Все они нуждаются как в оценке эффективности их защиты, так и в поиске неизвестных уязвимостей в них. Технология анализа защищенности исследует сеть и ищет слабые места в ней, обобщает эти сведения и печатает по ним отчет.

Если система, реализующая эту технологию, содержит и адаптивный компонент, то устранение найденной уязвимости будет осуществляться не вручную, а автоматически. Технология анализа защищенности является действенным методом, позволяющим реализовывать политику сетевой безопасности прежде, чем будет осуществлена попытка ее нарушения.

Обнаружение атак является процессом оценки подозрительных действий, происходящих в корпоративной сети. Обнаружение атак определяется с помощью анализа журналов регистрации ОС или сетевого трафика.

Адаптивный компонент модели адаптивного управления безопасностью отвечает за модификацию процесса защищенности.

Оценка риска состоит в выявлении и ранжировании уязвимостей (по степени серьезности ущерба потенциальных воздействий), подсистем сети (по степени критичности), угроз (исходя из вероятности их реализации) и т.д.

Поскольку конфигурация сети постоянно меняется, то процесс оценки риска должен производиться постоянно.

Использование модели адаптивной безопасности сети позволяет контролировать практически все угрозы и реагировать на них эффективным способом.

Список использованных источников:

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.: ил. — (Профессиональное образование)

2. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. - М.: ДМК Пресс, 2004. - 616 с.

3. Лукацкий А. Обнаружение атак (2-е изд.) . Серия "Мастер систем". - СПб.: БХВ-Петербург, 2003. - 608 с.: ил.

РАЗЛОЖЕНИЕ ФУНКЦИЙ В БАЗИСЕ ОРТОГОНАЛЬНЫХ ПОЛИНОМОВ ЧЕБЫШЕВА

Побудей П.П.

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

Власова Г.А. – к.т.н., доцент кафедры защиты информации

Данная работа содержит исследование свойств ортогональных полиномов, а именно полиномов Чебышева, а также разложение некоторых математических функций в базисе данных полиномов.

Для изучения свойств ортогональных полиномов и математических функций, их визуализации (рисунок 1), а также исследования разложения некоторых математических функций в базисе данных полиномов была создана программа на языке JavaScript.

В работе рассматривались следующие ортогональные полиномы:

Полиномы Чебышева (1, 2 рода) [1,2]:

$T_n(x) = \frac{(x+\sqrt{x^2-1})^n + (x-\sqrt{x^2-1})^n}{2}$ – полином Чебышева 1 рода;

$U_n(x) = \frac{(x+\sqrt{x^2-1})^{n+1} - (x-\sqrt{x^2-1})^{n+1}}{2\sqrt{x^2-1}}$ – полином Чебышева 2 рода;

Рисунок 1 – Визуализация на примере полинома Чебышева 1 рода.

При разложении функций в базисе полиномов Чебышева для расчета спектральных составляющих использовалось следующее выражение [1]:

$$c_n = \frac{2}{\pi} \int_{-1}^{1} \frac{f(x)\, T_n(x)}{\sqrt{1-x^2}}\, dx.$$

Функция sin(10x) и ее разложение в базисе полинома Чебышева 1 рода приведены на рисунках 2 и 3.

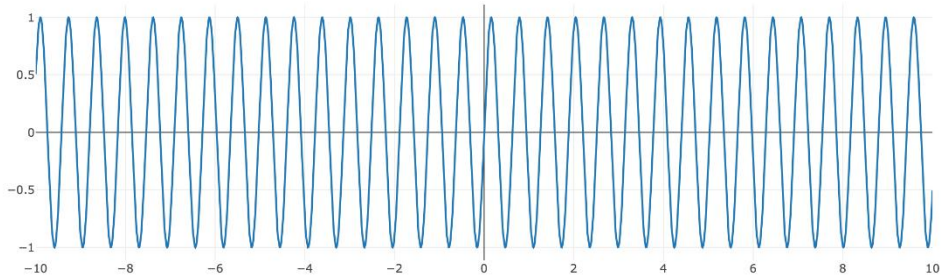


Рисунок 2 – Функция sin(10x)

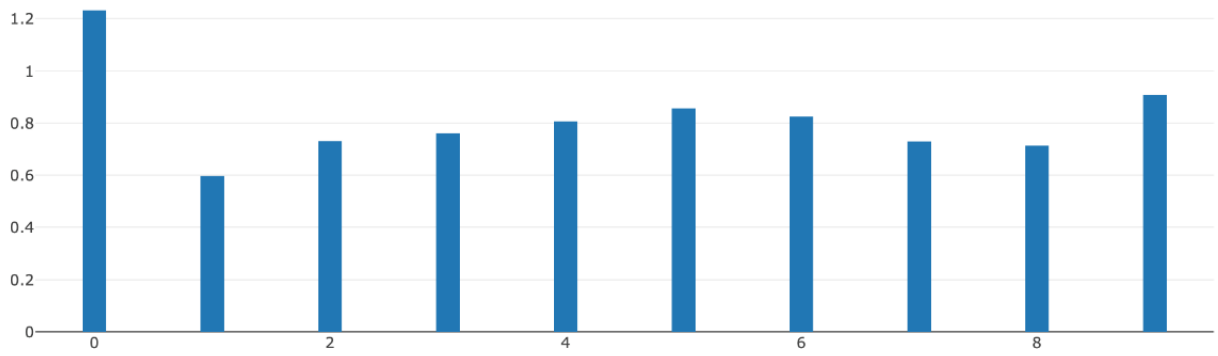


Рисунок 3 – Разложение функции sin(10x) в базисе полинома Чебышева 1 рода.

Программа предоставляет возможность разложения различных математических функций, например, sin(x)/x, и функции sin(10x)/(10x) (рисунок 4, 5).

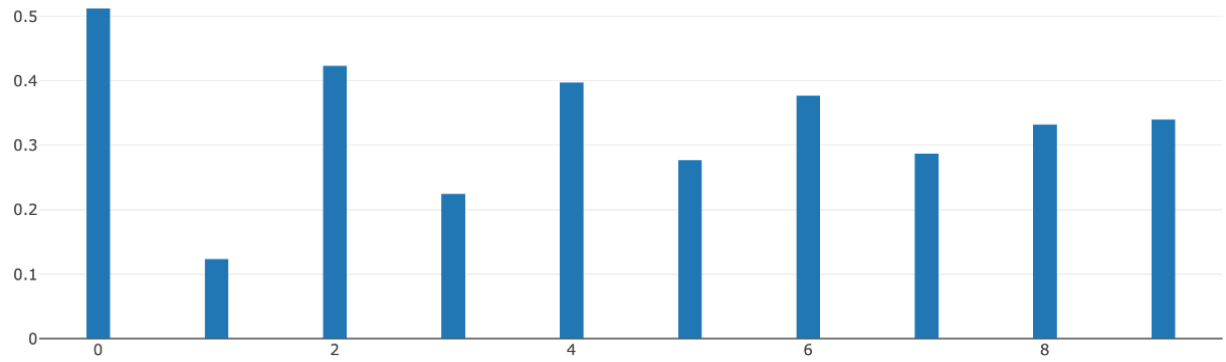


Рисунок 4 – Разложение функции sin(x)/x в базисе полинома Чебышева 1 рода.

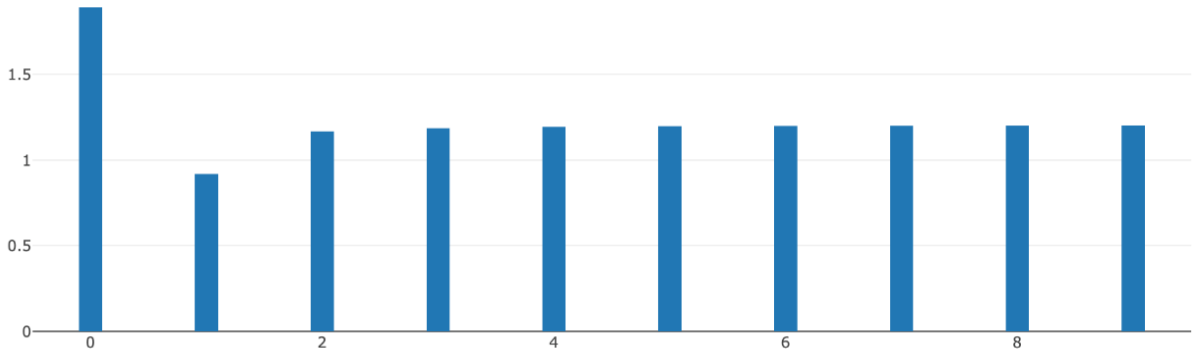


Рисунок 5 – Разложение функции sin(10x)/10x в базисе полинома Чебышева 1 рода.

Сравнение спектров рассмотренных функций показывает, что при увеличении аргумента функции происходит увеличение значений составляющих, а также наблюдается балансировка по значениям.

Список использованных источников:

12. И.С. Гоноровский: Радиотехнические цепи и сигналы. – М.: Радио и связь, 1986 г. – 512 с.

13. Chebyshev Polynomials [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.johndcook.com/ChebyshevPolynomials.pdf

РАЗЛОЖЕНИЕ ФУНКЦИЙ В БАЗИСЕ ПОЛИНОМОВ ЛЕЖАНДРА

Палиев О.А.

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

Власова Г.А. – к.т.н., доцент кафедры защиты информации

Работа содержит исследование свойств полиномов Лежандра, а также разложение математических функций в базисе данного полинома.

В процессе изучения полиномов Лежандра, визуализацию которых можно увидеть на рисунке 1, была написана программа на языке Python. Программа позволяет разложить математические функции в базисе данных полиномов.

Полиномы Лежандра определяются формулой [1, 2]:

$$P_n(x) = \frac{1}{2^{n*n!}} * \frac{d^n}{dx^n}(x^2-1)^n$$

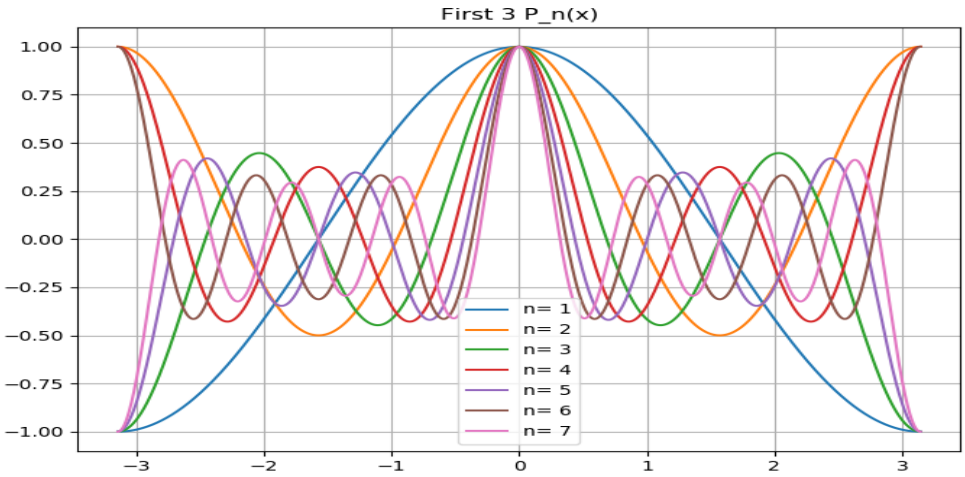


Рисунок 1 – Визуализация на примере полинома Лежандра

Для расчета спектральных составляющих в базисе этого полинома используется следующая формула[2]:

+

$$c_n = \frac{2n+1}{2}\int_{-1}^{1} f(x)P_n\,dx.$$

Примеры разложения некоторых математических функций в базисе полиномов Лежандра.

На рисунке 2 представлены вид довольно простой математической функции sin(x) и ее разложение в базисе полиномов Лежандра:

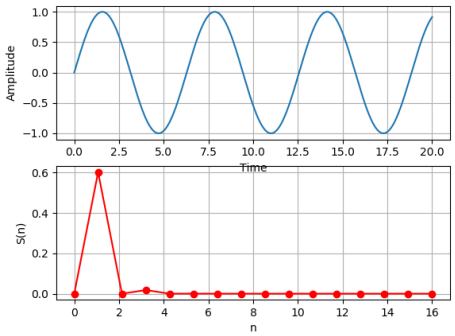


Рисунок 2 – Разложение функции sin(x)

Изменим первоначальную функцию на sin(10x) и посмотрим, как изменится сектор, рисунок 3:

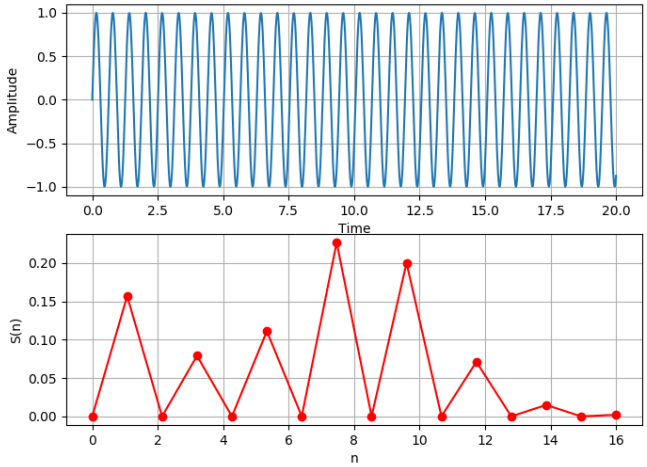


Рисунок 3 – Разложение функции sin(10*x)

Рассмотрим разложение функции экспоненты: , (рисунки 4 и 5):

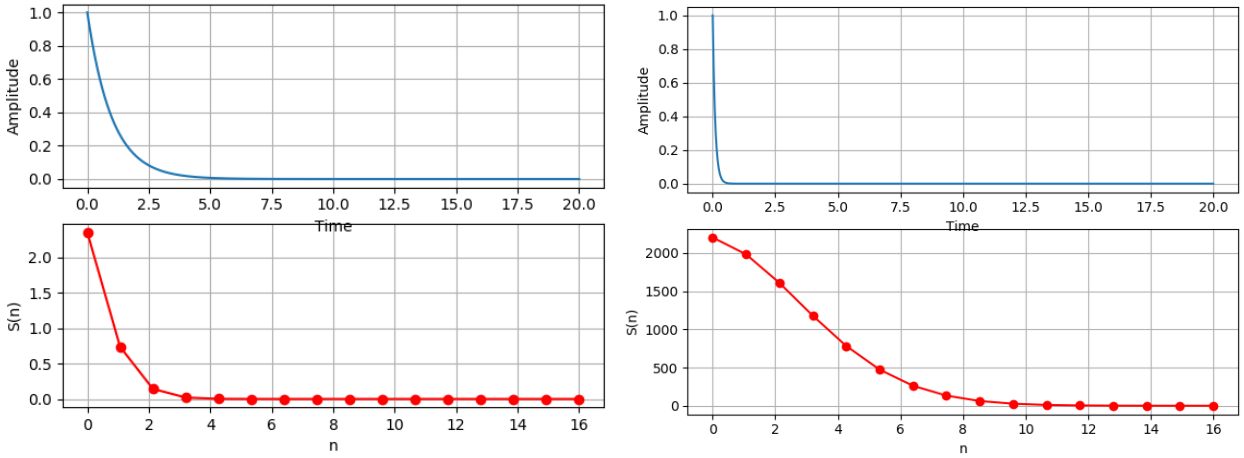


Рисунок 4 и 5 – Разложение функций ,

Также разложим более сложную функцию , рисунок 6:

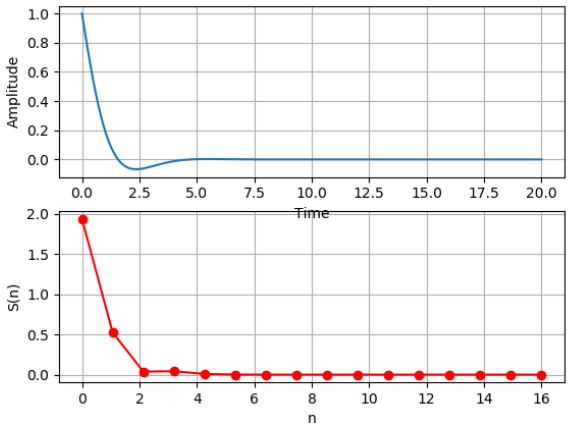


Рисунок 6 – Разложение функций

При сравнении спектров различных функций, можно заметить, что данный полином более подходит для разложения не периодичных функций.

Список использованных источников:

1. Legendre Polynomial [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.mhtlab.uwaterloo.ca/courses/me755/web_chap5.pdf
2. И.С. Гоноровский: Радиотехнические цепи и сигналы. – М.: Радио и связь, 1986 г. – 512 с.

ПРИМЕНЕНИЕ АДАПТИВНОСТИ В СИСТЕМАХ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

Мажейко А.М.

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

Белоусова Е.С. – к.т.н.,доцент

Статья представляет собой обзор проблемы классических систем аутентификации пользователей, а также рассматривает предмет использования адаптивной аутентификации пользователей в информационных системах. Приводится авторский взгляд на достоинства и недостатки обоих подходов в аутентификации.

Классическая система аутентификации построена на принципе предоставления средству контроля разграничения доступа секретного либо оригинального ключа. В данном случае предполагается, что секретный ключ знает только легитимный пользователь, либо этот же пользователь обладает артефактом доступа, не предполагающим возможность воспроизведения копий и изготовления подделки. Практика показывает ненадежность использования пароля по двум основным причинам: слабая устойчивость ко взлому и компрометация фразы пользователем.

Слабая устойчивость объясняется большим набором требований, предъявляемых к вновь создаваемому паролю. Пользователи дабы избежать случая забыть пароль используют простые фразы и комбинации. Ежегодно составляются рейтинги самых взламываемых паролей. Таким образом в открытый доступ попадают наиболее часто встречаемые секретные фразы. Автор книги [1] утверждает, что 4 % паролей попадают в первые 100 самых используемых паролей (рисунок 1).

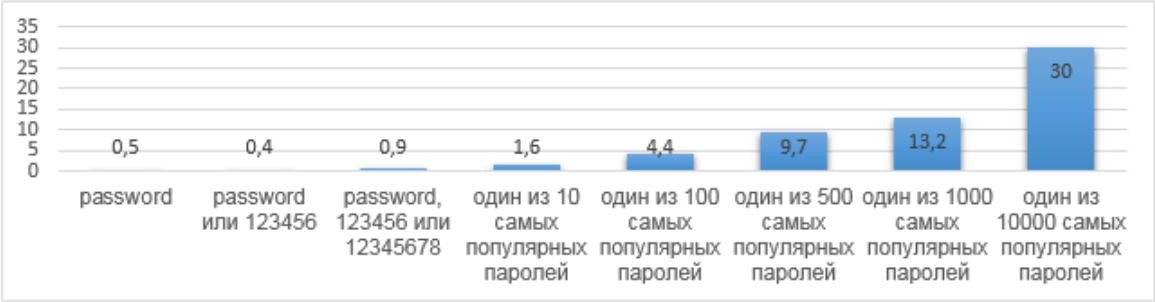


Рисунок 1 – Доли пользователей, использующих наиболее популярные пароли

Компрометация пароля также является частым явлением. В статистических данных [2] упоминается о нарушении правил конфиденциальности не менее чем у трети всех пользователей.

Разработчики систем защиты предлагают различные варианты решения данной проблемы. Один из способов – внедрение многофакторной аутентификации. По существу данный метод усложняет взлом системы, но не избавляет подход от ранее названных недостатков. Вводимые параметры как и ранее остаются статическими значениями. Поиск и внедрение динамических составляющих в процесс аутентификации представляется перспективным направлением развития.

В биометрии к динамическим параметрам относят поведенческие характеристики объекта. Здесь существует проблема повторного воспроизведения считываемых параметров. Неудачный выбор характеристик приведет к отказу в доступе. Доработка подобных систем привела исследователей к внедрению способности адаптации системы к считываемому субъекту.

Наиболее отличительной научной работой в данном направлении является диссертация Нестерука Ф.Г. [3]. Работа основана на применении нейронных сетей для аутентификации пользователя. В числе последних находится разработка система компании SABIGLOBAL. Компания позиционирует систему, обладающую самообучением на базе получаемого электромагнитного «отпечатка» структуры тела человека – реакции тела на излучение СВЧ- и КВЧ-диапазонов.

В соответствии с вышесказанным является перспективным разработка системы контроля доступа в виду необходимости подстройки механизма аутентификации под конкретного пользователя, отличающегося от существующих систем подходом считывания статических данных.

Список использованных источников:

14. XATO: Information Security by Mark Burnett[Электронный ресурс]. – Режим доступа: https://xato.net/10-000-top-passwords-6d6380716fe0. – Дата доступа: 24.06.2018.

15. Информационный портал ВЫБЕРИ!BY[Электронный ресурс]. – Режим доступа: https://viberi.by/news/banki/issledovanie_kazhdyj_tretij_polzovatel_seti_razglashaet_svoi_paroli. – Дата доступа: 12.01.2019.

16. Нестерук, Ф. Г. Разработка модели адаптивной системы защиты информации на базе нейро-нечеткихсетей :дис. канд. техн. наук : 05.13.19 / Ф.Г. Нестерук, – Санкт-Петербург, 2005. – 164 л.

МЕТОДИКА ПОСТРОЕНИЯ СИСТЕМЫ ВИДЕОАНАЛИТИКИ

Лабкович В.И., Петров С.Н.

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

Петров С.Н. – к.т.н., доцент

В работе приводится описание методики построения системы видеоаналитики.

Сегодня тематика интеллектуальных систем и решений очень популярна. Одним из ключевых направлений цифрового видеонаблюдения является видеоаналитика.

Видеоаналитика — технология, использующая методы компьютерного зрения для автоматизированного получения различных данных на основании анализа последовательности изображений, поступающих с видеокамер в режиме реального времени или из архивных записей. Видеоаналитика представляет собой программное обеспечение (ПО) для работы с видеоконтентом. В основе программного обеспечения лежит комплекс алгоритмов машинного зрения, позволяющих вести видеомониторинг и производить анализ данных без прямого участия человека [0].

Существует перечень классических задач, с которыми видеоаналитика успешно справляется, что подтверждено практическими результатами. Наиболее распространённые задачи следующие:

– распознавание номеров (автомобильных, на денежных купюрах, документах);

– обнаружение опасных ситуаций (скопления людей, оставленные предметы, возгорания и задымления и т. п.);

– распознавание человеческих лиц и поиск их в базах данных;

– распознавание с целью подсчёта людей и транспорта.

На рисунке 1 показана типовая схема системы видеоаналитики.

Рисунок 1 – Типовая схема системы видеоаналитики

Использование видеоаналитики дает возможность в автоматическом режиме, без участия человека, в процессе видеонаблюдения решать задачи, которые обычно под силу только человеческому зрению.

Различают 3 типа обработки видеопотока [2]:

1. Серверная видеоаналитика. Архитектура основана на централизованной обработке видеоконтента на сервере. При этом сервер анализирует видеопотоки от всех камер или кодеров и также может их записывать, но чаще всего сервер, анализирующий видео, – это отдельная машина под задачи только видеоанализа.

2. Распределённая видеоаналитика. Особенность архитектуры заключается в том, что обработка видеопотока распределена между источником видеоданных (камерой или кодером) и центральным оборудованием (сервером). Например, в системах многокамерного слежения обнаружение объектов и слежение производится в источнике видеоданных, а сопоставление результатов и между несколькими источниками, и трекинг осуществляется через сервер.

3. Встроенная в камеру видеоаналитика – реализуется непосредственно в источнике видеоданных, например, в видеокамере. Встроенный видеоанализ, как правило, работает на выделенном процессоре внутри видеоустройства и передает результаты (метаданные) параллельно с видеопотоком.

Пример работы видеоаналитики представлен на рисунке 2, в данном примере задействованы тепловизионная видеокамера (используемая для фиксации изменения температурного фона), PTZ-видеокамера с максимальным углом обзора 360 градусов, система оповещения тревожных ситуаций (громкоговоритель), средства передачи информации:

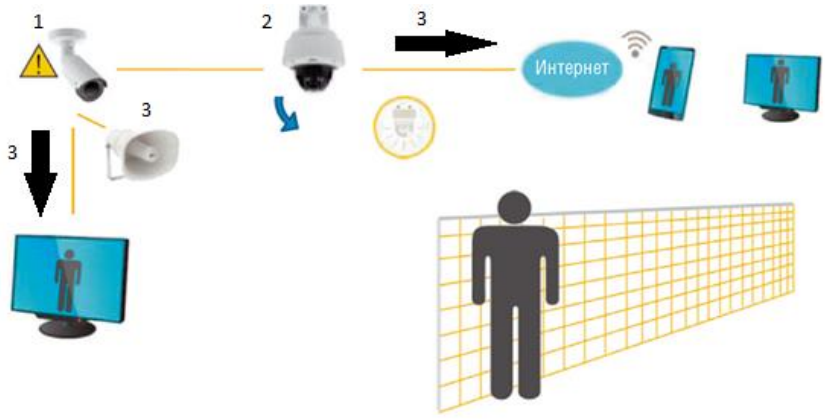


Рисунок 2 – Принцип работы системы видеоаналитики

При возникновении внештатной ситуации, например при пересечении охраняемого периметра потенциальным злоумышленником в ночное время, тепловизионная камера (1), которая его детектировала, отправляет сигнал поворотной камере (2), после получения которого та должна развернуться в указанном направлении. Автоматически отправляется оповещение (3) на мобильное устройство посредством сети GSM или рабочее место оператора с помощью проводных линий связи. Одновременно через громкоговоритель (3) транслируется звуковое предупреждение о том, что постороннему необходимо покинуть территорию. Как свидетельствуют данные alarm.org, подобным образом удается предотвратить до трех четвертей (74%) всех незавершенных вторжений. В этой схеме нет никакого компьютера, устройства общаются только между собой [3].

На рисунке 3 представлена схема работы системы видеоаналитики магазина, направленной на распознавание лиц.

Рисунок 3 – Схема работы видеокамеры для распознавания лиц

Современный мир становится более компьютеризированным. Системы машинного зрения будут развиваться и совершенствоваться вместе с ним. Этот сегмент представляет собой одно из приоритетных направлений разработок мировых исследовательских центров. Видеоаналитика широко применяется в бизнесе и обеспечении безопасности.

Список использованных источников:

1. Видеоаналитика [Электронный ресурс]. – Режим доступа: https://dic.academic.ru/dic.nsf/ruwiki/1767979

2. Видеоаналитические алгоритмы и детекторы [Электронный ресурс]. – Режим доступа: https://www.aktivsb.ru/statii/videoanaliticheskie_algoritmy_i_detektory.html

3. Видеонаблюдение не только для обеспечения безопасности[Электронный ресурс]. – Режим доступа: https://www.osp.ru/lan/2016/06/13049749/

РАЗЛОЖЕНИЕ ФУНКЦИЙ В БАЗИСЕ ПОЛИНОМОВ ЛАГЕРРА

Ефремов Д.О.

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

Власова Г.А. – к.т.н., доцент кафедры защиты информации

Работа содержит исследование свойств ортогональных полиномов Лагерра, а также разложение математических функций в базисе данных полиномов.

Для изучения свойств ортогональных полиномов и математических функций, их визуализации (рисунок 1), а также исследования разложения некоторых математических функций в базисе данных полиномов была создана программа на языке JavaScript.

В работе рассматривались ортогональные полиномы Лагерра, задаваемые формулой [1,2]:

$$L_n = \frac{e^x d^n}{n!\, dx^n} * (x^n e^{-x}), x \geq 0$$

Вид первых семи полиномов приведем на рисунке 1.

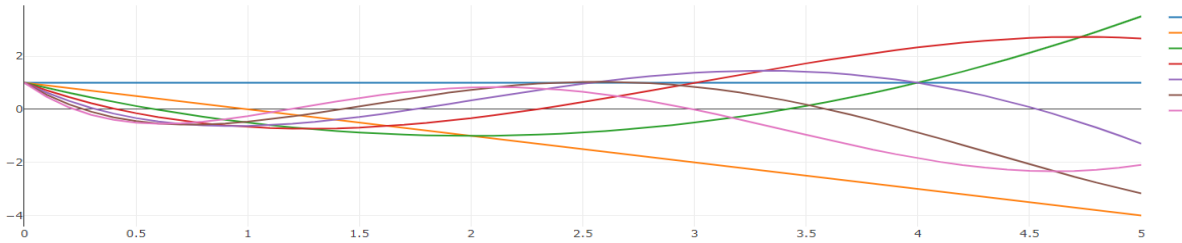


Рисунок 1 – Визуализация полинома Лагерра.

При разложении функций по полиномам Лагерра спектральные коэффициенты должны определяться по формуле[1]:

$$c_n = \int_0^{\infty} f(x) * e^{-\frac{x}{2}} * L_n(x)$$

Визуализация функции cos(5x) и ее разложение в базисе полинома Лагерра приведены на рисунках 2, 3.

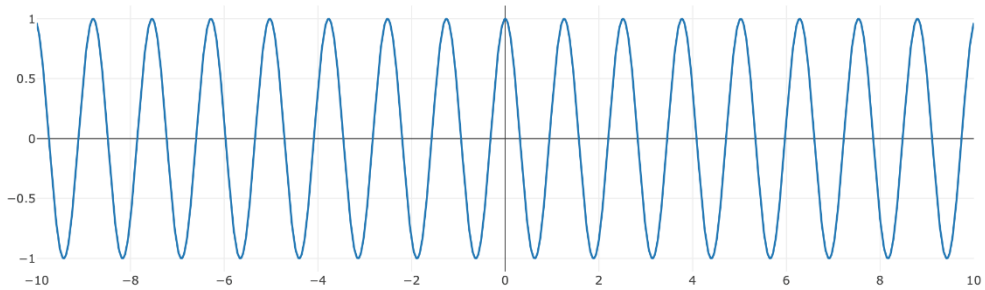


Рисунок 2 – Функция cos(5x).

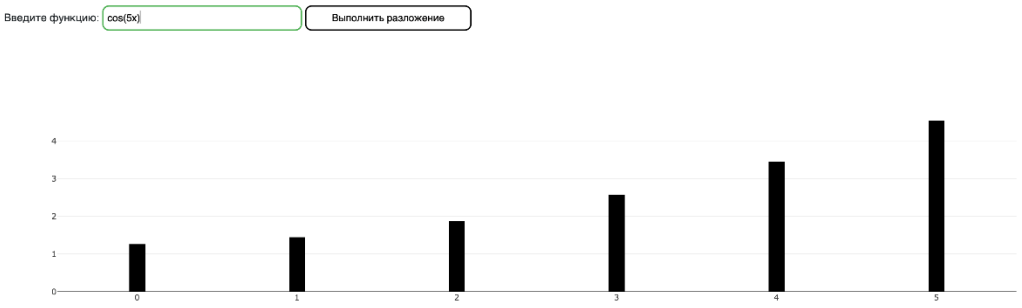


Рисунок 3 – Разложение функции cos(5x) в базисе полинома Лагерра.

Программа предоставляет возможность разложения различных математических функций, например, cos(x)/x, и функции cos(5x)/(5x) (рисунок 3,4).

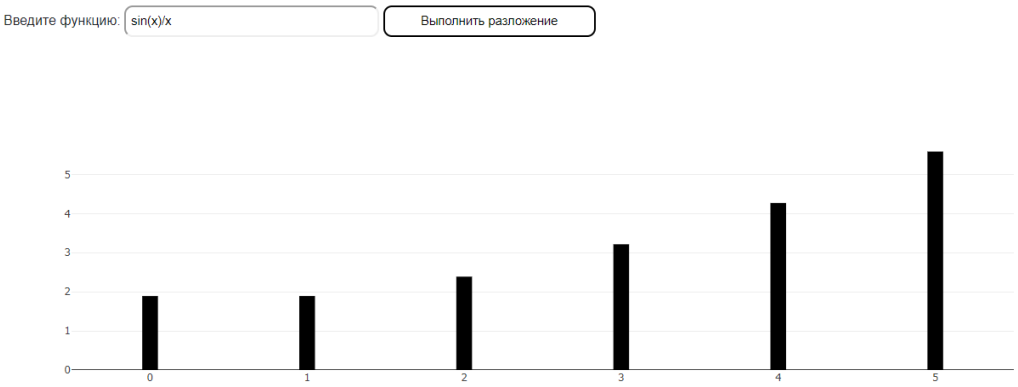


Рисунок 4 – Разложение функции cos(x)/x в базисе полинома Лагерра.

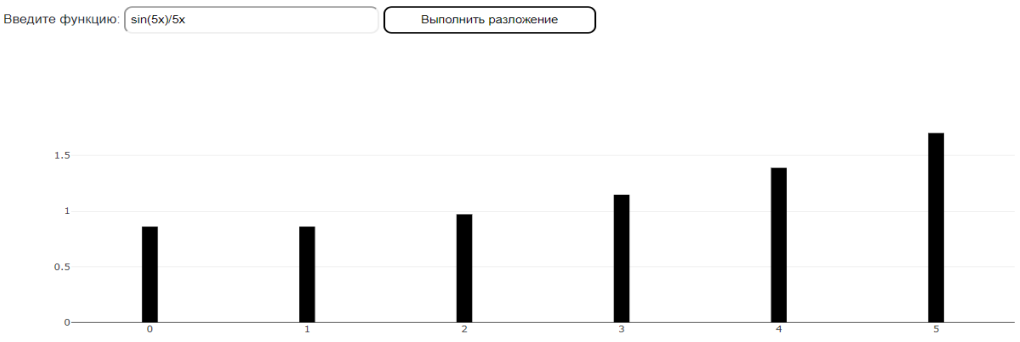


Рисунок 5 – Разложение функции cos(5x)/5x в базисе полинома Лагерра.

Сравнение двух спектров рассмотренных функций показывает, что при увеличении аргумента функции происходит уменьшению значений составляющих.

Список использованных источников:

1. И.С. Гоноровский: Радиотехнические цепи и сигналы. – М.: Радио и связь, 1986 г. – 512 с.
2. Laguerre Polynomials [Электронный ресурс]. – Электронные данные. – Режим доступа: https://archive.lib.msu.edu/crcmath/math/math/l/l042.htm

ЗАЩИТА ГОЛОСОВОЙ ИНФОРМАЦИИ В СЕТЯХ ПОДВИЖНОЙ РАДИОСВЯЗИ

Дударенков А.О., Зельманский О.Б.

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

Зельманский О.Б. – к.т.н.,доцент

Для защиты речевой информации в сетях подвижной радиосвязи предлагается программно-аппаратный модуль, обеспечивающий предварительное шифрование речевой информации до ее передачи на мобильное устройство и соответствующее дешифрование на выходе принимающего мобильного устройства.

В настоящее время тема обеспечения конфиденциальности речевой информации при использовании сетей подвижной радиосвязи остается одним из проблемных пунктов в организации информационной безопасности. В связи с чем, защита речевой информации в сетях подвижной радиосвязи является повседневной задачей. В большинстве случаев данная задача решается путем шифрования речевой информации на основе программных средств, что не позволяет подтвердить отсутствие незадекларированных возможностей и оценить их эффективность. Таким образом, задача защиты речевой информации, передаваемой по сетям радиосвязи, является весьма актуальной.

Исследование стандартов мобильной связи GSM, UTMS, LTE, целью которого был анализ инструментов обеспечения безопасности переговоров, показало большое количество существующих уязвимостей в алгоритмах шифрования, ставящих под угрозу вопрос конфиденциальности информации во время разговора. Использование базисных компонентов кодирования речи, таких как скремблеры или вокодерные системы, возможно в совокупности с криптографическими алгоритмами с целью имитации шума для дополнительного снижения разборчивости речи.

Соответственно для защиты речевой информации предлагается программно-аппаратный модуль, который подключается к мобильному устройству связи и осуществляет шифрование речевого сигнала до его непосредственной подачи в мобильное устройство.

При разработке программно-аппаратного модуля были изучены уже имеющиеся мировые аналоги, опыт и методы обеспечения безопасности переговоров популярными производителями смартфонов [1-7]. Исследование операционной систем Android показало, что в ней практически не имплементированы какие-либо инструменты защиты информации и имеется много уязвимостей, связанных с получением прав полного доступа к ядру. В свою очередь операционная система iOS позволяет осуществлять процессинг программ на виртуальной машине [8].

Первым этапом разработки стало создание программного модуля, обеспечивающего шифрование и дешифрование речевого сигнала. Для этого была применена библиотека классов NAudio на базе языка программирования C#. Тестирование программного модуля выглядит следующим образом. Исходный аудиофайл, содержащий речь, загружается в программное средство Wave Viewer и воспроизводится акустической системой. Данные, загруженные и отображаемые в средстве Wave Viewer, шифруются, а результаты сохраняются в аудиофайле. После этого данный аудиофайл, содержащий зашифрованный сигнал, также загружается в программное средство Wave Viewer, воспроизводится и записывается с помощью микрофона уже другого персонального компьютера или телефона. Затем записанный зашифрованный аудио сигнал расшифровывается, загружается в программное средство Wave Viewer и воспроизводится акустической системой.

Вторым этапом является разработка аппаратной составляющей с целью установки на нее разработанного программного модуля, что позволит получить независимый программно-аппаратный модуль совместимый с большинством мобильных устройств.

Список использованных источников:

17. Архитектура BlackBerry [Электронный ресурс]. – Режим доступа : https://us.blackberry.com/enterprise/blackberry-connect/.

18. Техника для спецслужб. Крипто смарт телефон «Cancort» [Электронный ресурс]. – Режим доступа : www.sis-tss.ru/2010-06-26-06-44-58/7817-kripto-smart-telefon-cancort.html.

19. Технология криптофон [Электронный ресурс]. – Режим доступа : www.cryptophone.de/en/background/cryptophone-technology/encryption-engine/

20. Скремблер «Guard Bluetooth» компании «Логос» [Электронный ресурс]. – Режим доступа : http://www.shpionam.net/skrembler-guard-bluetooth.html.

21. Техника для спецслужб. Устройство для защиты разговоров по смартфону «Референт PDA» [Электронный ресурс]. – Режим доступа : http://www.bnti.ru/des.asp?itm=3630&tbl=04.03.05.02.

22. Техника для спецслужб. Криптотелефон «StealthPhone» [Электронный ресурс]. – Режим доступа : www.bnti.ru/des.asp?itm=6220&tbl=04.03.07.02.

23. Aparna R. A Review on Cryptographic Algorithms for Speech Signal Security / Chitra D. P. // ITETICS – 2016 – №5.

24. Стандрат iOS11 2018 [Электронный ресурс] : Datasheet / Apple. – Режим доступа : https://apple.com/business/docs/iOS_Security_Guide.pdf.

РАСШИРЕНИЕ БАЗОВОГО ФУНКЦИОНАЛА MALTEGO С ПОМОЩЬЮ ФРЕЙМВОРКА CANARI

Давлатов Ш.Р.

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

Кучинский П.В. – доктор технических наук

Сбор и анализ информации является неотъемлемой частью любого качественного аудита информационной безопасности автоматизированных систем. В данной работе рассматривается инструмент Maltego, который широкоприменяетсядля сбора данных и автоматического построения связей между различными объектами исследования. Приводится пример расширения базового функционала Maltego с помощью фреймворкаCanari на основе языка программирования Python.

Maltego является проприетарным программным обеспечением, который используются для построения и анализа связей между различными объектами информационной системы. Его особенностями являются: визуализирование, обработка и комбинирование информации для более детального анализа данных, полученных из открытых источников информации. С помощью Maltegoможно также проводить автоматический анализ источников данных с целью построения взаимосвязей между обнаруженными объектами (люди, профили социальных сетей, электронные почты, организации, документы, картинки,геолокации, веб-сайты, домены, DNS имена, IP адреса и другие интернет инфраструктуры). Данный инструмент широко используется специалистами по информационной безопасности на начальных этапах проведения аудита информационной системы:сбор первичнойинформации;автоматизацияпроцессаанализа данных; тестирование объекта защитына проникновение (например, для определенной сети организации нужно выявить - какиеданные доступны в открытом доступе внешнему миру: порты, IPадреса, NS записи и другие). Данная информация в руках злоумышленников может представлять значительный рискдля автоматизированной системы организации [1].

В основе работыMaltego лежит идея создания трансформаций, принцип работы которой напоминает функцию от одного аргумента.Результатом применения трансформациинад входным объектом должен быть набор (один илинесколько)выходных Maltego-сущностей. Таким образом, создается граф зависимостей между объектами исследования, узлы которой находятся в соотношении 1:1 (один к одному) или1:n (один ко многим).Самым главным преимуществом программы Maltegoявляется возможность гибкой настройки и адаптации под любые уникальные требования [2]. Один из вариантов расширения базового функционала Maltegoявляется использование фреймворкаCanari (исходный код доступенв открытом видена веб-сервисеGitHub: *https://github.com/redcanari/canari3*).Данный фреймворк распространяется под лицензией GNU (GeneralPublicLicense) v3.0,что дает пользователям все права для копирования, модифицирования и распространения программы. Рассмотрим пример построения новой Maltego-трансформации(рисунок 1), которая на вход принимаетдоменное имя и на выходе генерирует новые сущности: IP адрес, NSсервер и список похожих доменов.

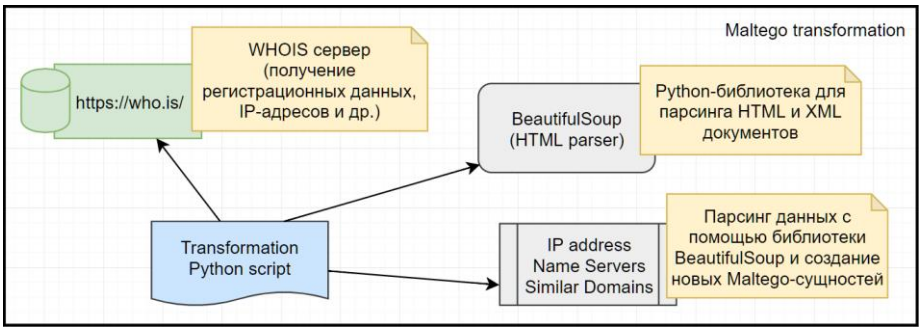


Рисунок 1 –Архитектура новой трансформации для Maltego

Для создания новой трансформации на базе фреймворкаCanari, необходимо создать Pythonкласс, который содержит обязательный метод *do_transform* [3]**.** Базовая логика трансформации должна быть реализована в даннойфункции. Рассмотрим детально алгоритм работы метода *do_transform*:

```
url = 'https://who.is/whois/' + request.entity.value
html_doc = urlopen(url).read()
soup = BeautifulSoup(html_doc, 'html.parser')
```

Сначала отправляется запрос на *who.is*сервер (в нашем примере, данный ресурс является основным источником информации), для получения регистрационных данных о домене. Ответ сервера записывается в переменной *html_doc*какhtml-документ и с помощью библиотеки *BeautifulSoup*парсится для дальнейшего доступа к его узлам в императивном стиле.Применяястандартныеметоды*find*и *find_all,*можно найти в документе теги с заданным условием поиска. Вторым аргументом передается лямбда-функция, которая ищет вхождение заданной строки (*'/nameserver' и '/whois-ip'*) в ссылке тега. Таким образом, мы получаем NSсервер,IPадрес и список похожихадресов, которые соответствуют входному домену:

```
ns = soup.find('a', href=lambda href: href and '/nameserver' in href)
ip = soup.find('a', href=lambda href: href and '/whois-ip' in href)
similar_domains = soup.find_all('a', href=lambda href: href and '/whois/bsuir' in href)
```

Для генерации новыхвыходных объектовMaltegonеобходимо конкатенировать аргумент*response*с новыми созданными сущностями. Из стандартной библиотеки Canariимпортируютсяфункции-генераторы *URL и IPv4Address*. На вход каждой функции передается текстовое представление имениNSсервера, IPадреса и списка доменов для генерации соответствующих сущностей на выходе:

```
response += URL(ns.text)
response += IPv4Address(ip.text)
for domain in similar_domains:response += Domain(domain.text)
```

Последней инструкцией функции*do_transform*обязательно должнобыть возвращение результата -*returnresponse.* Для того, чтобы протестировать работу данного скрипта необходимо выгрузить его для программы Maltego путем набора команды *canaricreate-profiledemo*в терминале операционной системы, где *demo*является именем корневой папки проекта.

Для проверки результата применения трансформации, в новой вкладке Maltegonужно создать входную сущность - доменное имя (в качестве примера введем *bsuir.by)*. Как видно из рисунка 2 – разработанная функцияна выходе генерирует сущности трех типов: NSсервер с найденным значением *ns.bsuir.by*, IPадрес сервера, который обслуживает домен – *46.216.181.36*, а также, список доменовс префиксом *bsuir-*. Для более детального анализа, можно запустить созданную трансформацию для всех выходных доменов по отдельности. Maltegoавтоматически построит все взаимосвязи между объектами с подробной информацией о соединениях.

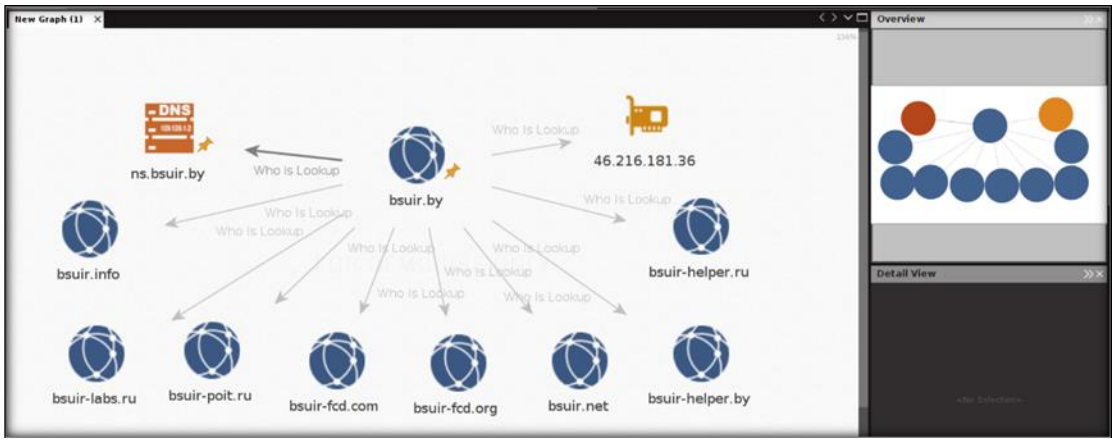


Рисунок 2 – Результат применения новой трансформации для Maltego

Таким образом, в данной работе был рассмотренинструмент для сбора и анализа данныхMaltego, который широко используется в сфере компьютерной безопасности. Предлагаемый вариант расширения базового функционала на базе фреймворкаCanariпозволяет с легкостью настроить программу под любые уникальные требования, которые необходимы специалистам по информационной безопасности для проведения более качественного и детального аудита безопасности информационных систем.

Список использованных источников:

25. ДавлатовШ.Р. Система сбора, анализа и визуализации данныхоб устройствах в сети Интернет // Доклады БГУИР, № 6, 2018, С. 19-25.

26. MaltegoOSINTBlog [Электронный ресурс], режим доступа: https://maltego.blogspot.com – Дата доступа: 08.02.2019

27. CanariFramework'sdocumentation[Электронный ресурс], режим доступа: http://www.canariproject.com/en/latest/ – Дата доступа: 05.02.2019

ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК С ПОМОЩЬЮ HONEYPOT

Грицкевич В.И., Петров С.Н.

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

Петров С.Н. – к.т.н., доцент

В работе приводится описание полуавтоматического подхода к обнаружению атак с помощью ханипота совместно с человеческими возможностями принятия решения.

В современном мире для любой организации очень важно защитить свои активы от нападения злоумышленников. Чтобы осуществить мечту о полной безопасности, нужно быть на шаг впереди злоумышленников, или необходимо определить возможную атаку, прежде чем она будет осуществлена. Одним из таких инструментов для мониторинга поведения злоумышленников является ханипот.

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 [1].

Целью 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.

Современный ханипот может включать в себе такие функции, как обнаружение фактов сканирования сети, мониторинг производительности, анализ журнала и т. д. для эффективного анализа поведения злоумышленника и принятия определенных решений, например, разрешить или заблокировать активность злоумышленника.

Архитектура рассматриваемой системы (рисунок 1) состоит из четырех различных компонентов, а именно: внешний брандмауэр, ханипот (виртуальная машина), база данных и специальная группа SOC (Security operating center, центр реагирования на инциденты информационной безопасности) для ручного анализа журналов. В ней присутствуют различные модули для определения наиболее точных результатов, которые помогут администратору принимать решения на основе генерируемых журналов. Данная архитектура состоит из следующих модулей: межсетевой экран, виртуальная машина (ханипот), база знаний, анализ IP, свод правил, группа SOC (центр реагирования на инциденты информационной безопасности) [2]. Внутреннее устройство ханипота представлено на рисунке 2.

Группа SOC (Security Operation Center) – это группа лиц, которые вручную анализируют данные из различных источников и подводят итоги для какого-либо действия или события с точки зрения уровня серьезности. Основным преимуществом команды SOC является следование полуавтоматическому подходу, заключающемуся в комбинировании автоматического и глубокого ручного анализа любого злонамеренного инцидента и приближении к нулевой вероятности ложных срабатываний.

Правило – это, по сути, протокол, которому будет следовать межсетевой экран для подавления злонамеренных действий. Свод правил – это набор как стандартных, так и настраиваемых правил, которые межсетевой экран будет автоматически извлекать через определенные промежутки времени. Помимо стандартных правил, которые брандмауэр будет вставлять на этапе инициализации, команда SOC также может обновлять правила на основе различных сценариев.

Система использует два типа межсетевых экранов, а именно: сетевой межсетевой экран и хостовой межсетевой экран (iptables), которые отвечают за обработку таких задач, как фильтрация

пакетов, сегрегация сети и предотвращение вторжений. Сетевой брандмауэр используется для сегрегации сети, разделяющей ханипот, SOC и сеть базы данных [2].

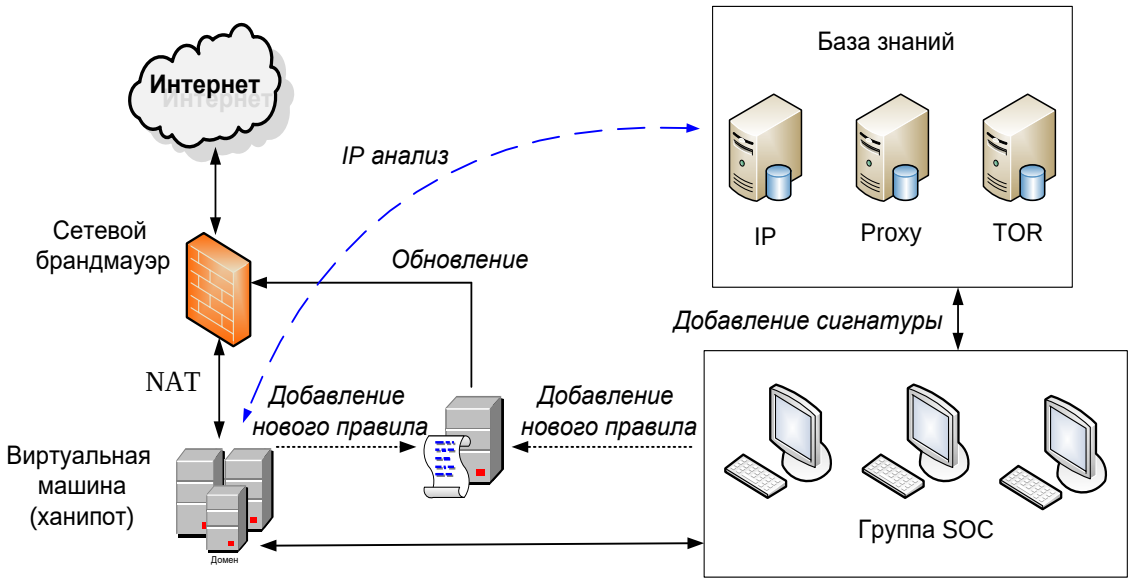


Рисунок 1 – Архитектура рассматриваемой системы

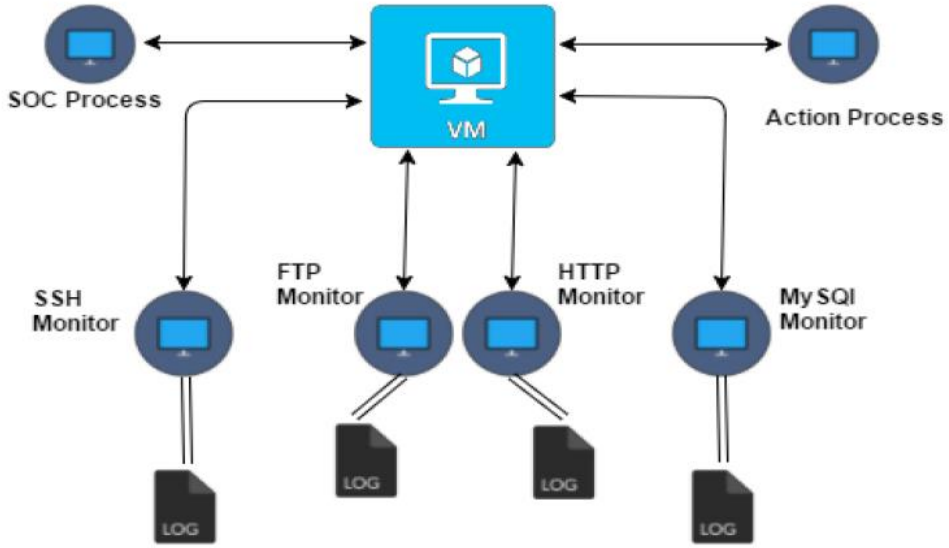


Рисунок 2 – Внутреннее устройство ханипота

Таким образом, основная цель заключается в создании самодостаточной децентрализованной системы для наблюдения за поведением злоумышленника с использованием полуавтоматического подхода. Предлагаемая система может преодолеть проблемы, имеющиеся в предыдущих реализациях, а именно минимизировать ложные срабатывания, путем выполнения ручного анализа. Система включает в себя логику для выполнения базового анализа поведения путем мониторинга различных путей к файлам и типов запросов в течение определенного периодического интервала, чтобы различать обычные и вредоносные действия конечного пользователя. Система также включает в себя взаимодействие с человеком и проверку данных с различных онлайн-ресурсов для получения наиболее точных результатов.

Список использованных источников:

1. Ханипот (Honeypot). [Электронный ресурс]. – Режим доступа: https://encyclopedia.kaspersky.ru/glossary/honeypot/.

2. Rahul koul, J. W. Bakal, Modern attack detection using intelligent honeypot, журнал «International research journal of engineering and technology», 2017, №4, p. 2866 – 2869.

АНАЛИЗ И МЕТОДЫ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ ОТ АТАК ТИПА LDAP-ИНЪЕКЦИЯ

Бодров В.А, Белоусова Е.С.

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

Белоусова Е.С. – к.т.н., доцент

В работе приводятся результаты анализа LDAP-инъекций и методов защиты веб-приложений от данного типа атак. Данный метод можно использовать для защиты любых веб-приложений.

В настоящее время огромную популярность получили веб-приложения, что обусловлено доступностью из любой точки мира, кроссплатформенностью и простотой в обновлении. Разработчики данных приложений в первую очередь уделяют внимание функциональности приложения, а не обеспечению безопасности своих разработок.

Lightweight Directory Access Protocol (LDAP) – это сетевой протокол прикладного уровня модели TCP/IP, используемый для доступа к службам каталогов. Наиболее широко используемыми реализациями служб LDAP являются Microsoft ADAM и OpenLDAP [1]. Служба каталогов LDAP представляет собой древовидную структуру, которая хранит и систематизирует информацию по общим атрибутам. Операции над каталогом, в частности, запись, чтение, сравнение осуществляется с помощью фильтров, которые определены в RFC 4515. При работе с веб-приложениями, использующих LDAP используются три основных вида запросов:

1) запрос без логических операторов;
2) запрос с использованием логического оператора «И»;
3) запрос с использование логического оператора «ИЛИ».

Ниже приведен пример простейшего LDAP запроса с использованием логического оператора «ИЛИ»:

$$(|\,(attribute1 = parameter1)(attribute2 = parameter2)).$$

Недостаточное внимание к фильтрации вводимых данных пользователя веб-приложения ведет к возможности использования LDAP-инъекции. Данные атаки основаны на тех же методах, что и атаки с использованием SQL. Следовательно, основная концепция атак заключается в использовании параметров, веденных пользователем, для модификации исходного LDAP запроса [2].

Предположим, что приложение создает запрос, с использованием логического оператора «И», для поиска в каталоге LDAP имени пользователя и соответствующего ему пароля с целью проведения процесса аутентификации. В качестве вводимых данных выступает имя пользователя (uname) и пароль пользователя (pwd). В данном случае запрос будет выглядеть таким образом:

$$(\&(username = uname)(password = pwd)).$$

Если злоумышленник вводит правильное имя пользователя, например, «alexander», а затем вводит определенную последовательность, то проверку пароля можно обойти. Представленный ниже запрос основан на изменение значения «uname» на значение «alexander)(&))» и добавлении любой строчки в качестве значения «pwd»:

$$(\&(username = alexander)(\&))(password = pwd))$$

Приложение обрабатывает только первую часть запроса, то есть

$$(\&(username = alexander)(\&)),$$

которое всегда является истинным выражением. Таким образом, злоумышленник получит несанкционированный доступ к системе без ввода пароля.

Предположим, существует некая поисковая система, позволяющая получить информацию о пользователях (имя пользователя, время регистрации в системе, время последнего входа и т. п.). Данный поисковый запрос к каталогу LDAP может быть выполнен с использованием логического оператора «ИЛИ»:

$$(|\,(param = username)(param = registration\_time)).$$

Используя LDAP инъекцию, злоумышленник может манипулировать данными, возвращаемыми от приложения. Если злоумышленник в качестве значения поля «param» отправит выражение «alexander)(uid=*)», то запрос будет иметь следующий вид:

$$(|\,(param = alexander)(uid = *))(param = registration\_time)).$$

Специальный символ «*» можно использовать для замены одного или нескольких символов в конструкции фильтра. В результате запроса приложение вернет злоумышленнику всех пользователей системы.

Как и в случае с SQL инъекцией, LDAP инъекция может быть «слепой». Под «слепой» понимается инъекция, при которой приложение не будет отображать все поля записей или сообщения об ошибках. В этом случае злоумышленник может использовать данное поведение для проведения успешных LDAP инъекций.

Предположим, что у нас есть приложение, которое в результате ввода имени пользователя работника организации «uname», отображает адрес его электронной почты. Наш запрос к приложению примет следующий вид:

$$(\&(username = uname)(objectClass = employee))$$

В случае отправки имени пользователя, которого не существует, мы получим соответствующее сообщение. Данное поведение может быть использовано для получения различных данных о пользователе, например, его пароля. Может использоваться метод перебора символов с использованием специального символа «*». При использовании инъекции в поле «username» равной «alexander)(userPassword=a*». Конечный запрос с инъекцией будет выглядеть следующим образом:

$$(\&(username = alexander)(userPassword = a*)(objectClass = employee))$$

В случае если пароль пользователя «alexander» начинается с буквы «a», мы получим ожидаемый ответ на правильный запрос, а именно, адрес электронной почты пользователя. Таким образом мы можем перебирать все символы до тех пор, пока не получим полноценный пароль пользователя «alexander».

Поскольку данный тип атаки выполняется на уровне приложений, межсетевые экраны и механизмы обнаружения вторжений, работающие на сетевом уровне, не могут предотвратить атаку. Однако общие рекомендации безопасности для служб каталогов LDAP могут уменьшить вероятность возникновение данной уязвимости: отключение индексирования полей, использование принципа минимальных привилегий и. т. д.

Разработчики не осведомлены о подобных инъекциях, поскольку на сегодняшний день существует довольно малое число информационных статей, посвященных данному типу атак. Быстрый поиск «LDAP» на ресурсах с открытым исходным кодом приложений, позволяет обнаружить большое количество приложений, уязвимых к атакам типа LDAP-инъекция.

Сегодня, инструменты статического анализа кода не готовы обнаруживать в коде данные уязвимости. Таким образом, разработчик, не разбирающийся в методах обеспечения безопасности, легко создаст уязвимый код.

Однако для предотвращения LDAP инъекций достаточно использовать фильтрацию вводимых данных пользователя. Для правильной фильтрации данных, поступающих в веб-приложение, разработчики должны обращать внимание только на десять специальных символов «|, &, (,), *, <,>, =, ~,!». Если разработчик отфильтровывает эти символы, атаки типа LDAP-инъекции работать не будут [3].

Таким образом, в работе рассмотрены основные принципы атаки на веб-приложения типа LDAP-инъекция и основные методы защиты от нее. В дальнейшей работе планируется разработать программное обеспечение, позволяющее обнаруживать и эксплуатировать данный тип уязвимости.

Список использованных источников:

1.Об Интернете, информационных технологиях и не только. [Электронный ресурс]. – Режим доступа: https://www.styler.ru/styler/ldap-injection/.

2.E. Guillardoy, F. Guzman, H. Abbamonte. LDAP Injection. Attack and Defence Techniques, журнал «HITB Magazine», 2010, №1, с. 9 – 17.

3.Vulners – Vulnerability Data Base. [Электронный ресурс]. – Режим доступа: https://vulners.com/static/appercut/ru/Java/InjectionLdap.html.

РАЗЛОЖЕНИЕ СИГНАЛОВ В БАЗИСЕ ФУНКЦИЙ УОЛША

Азаров А.В., Чернявский Н.С.

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

Власова Г.А. – к.т.н., доцент кафедры защиты информации

Данная работа содержит исследования разложения сигналов по функциям Уолша и примеры получения спектров различных сигналов в базисе данных функций.

Для данной работы была написана программа на языке C#, которая позволяет по заданному сигналу и его длительности получить спектр функции в базисе функций Уолша. Программа использует 16 функций Уолша (w0-w15). Разработанная программа также позволяет проводить упорядочение по Уолшу, Адамару или Пэли [1].

Для примера работы программы были выбраны следующие функции:

1) $S(t) = \sin(t)$ (см. Рисунок 1);
2) $S(t) = e\text{^}\sin(t)$ (см. Рисунок 2);
3) $S(t) = e^{-t} * t * \cos(t)$ (см. Рисунок 3).

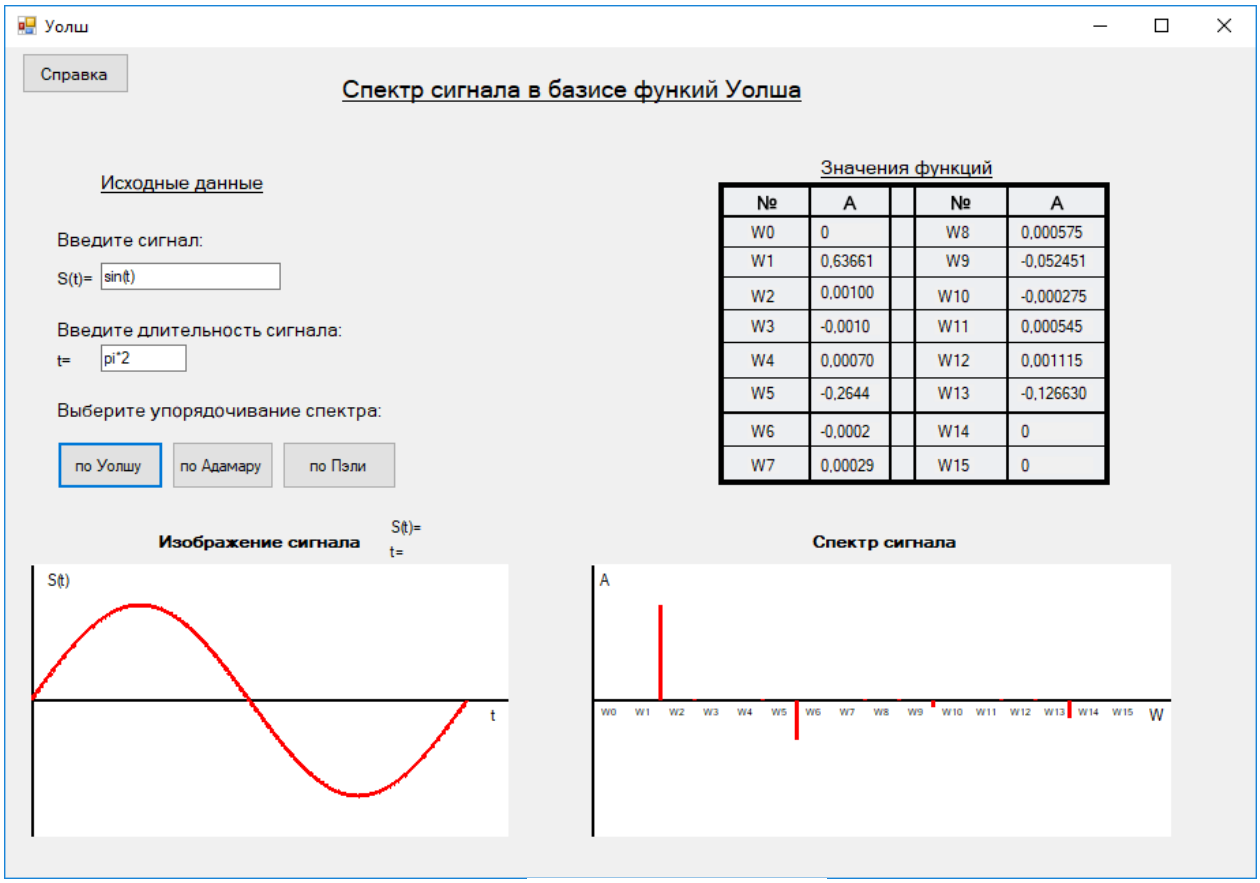


Рисунок 1 – Разложение функции sin(t)

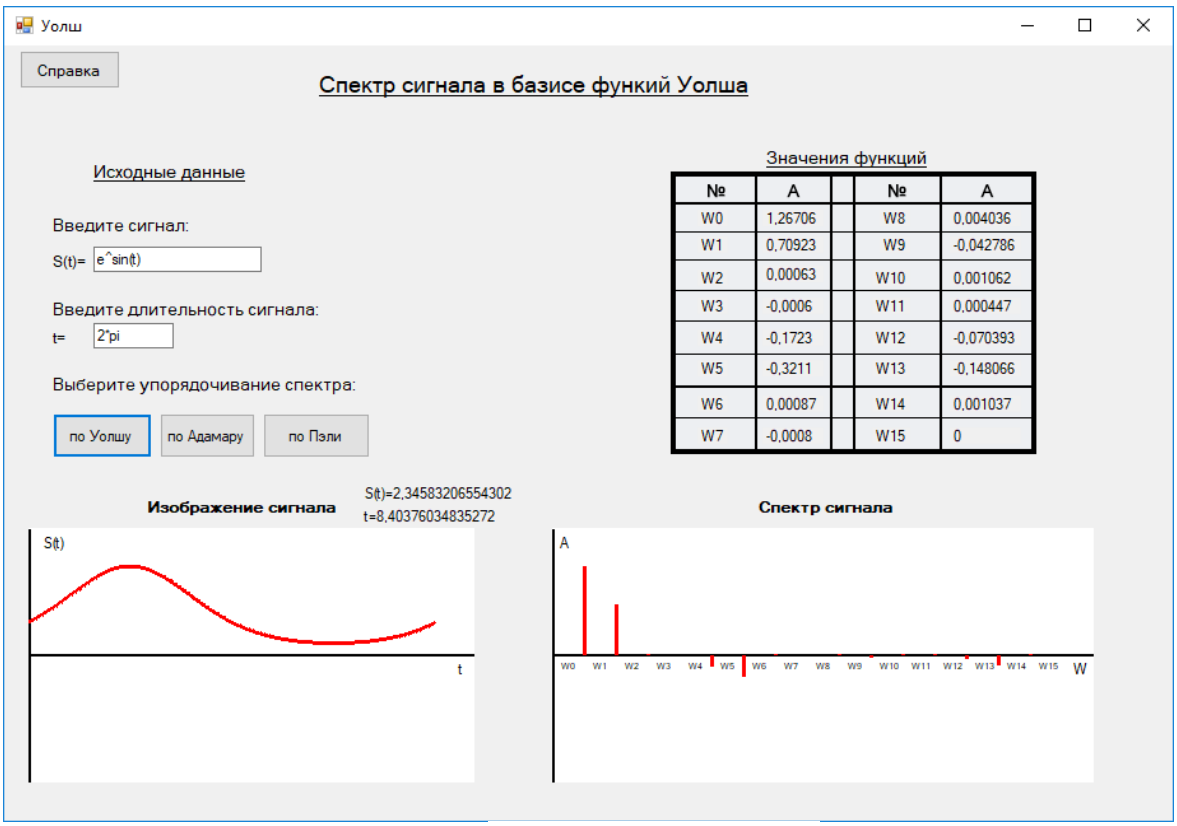


Рисунок 2 – Разложение функции e^sin(t)

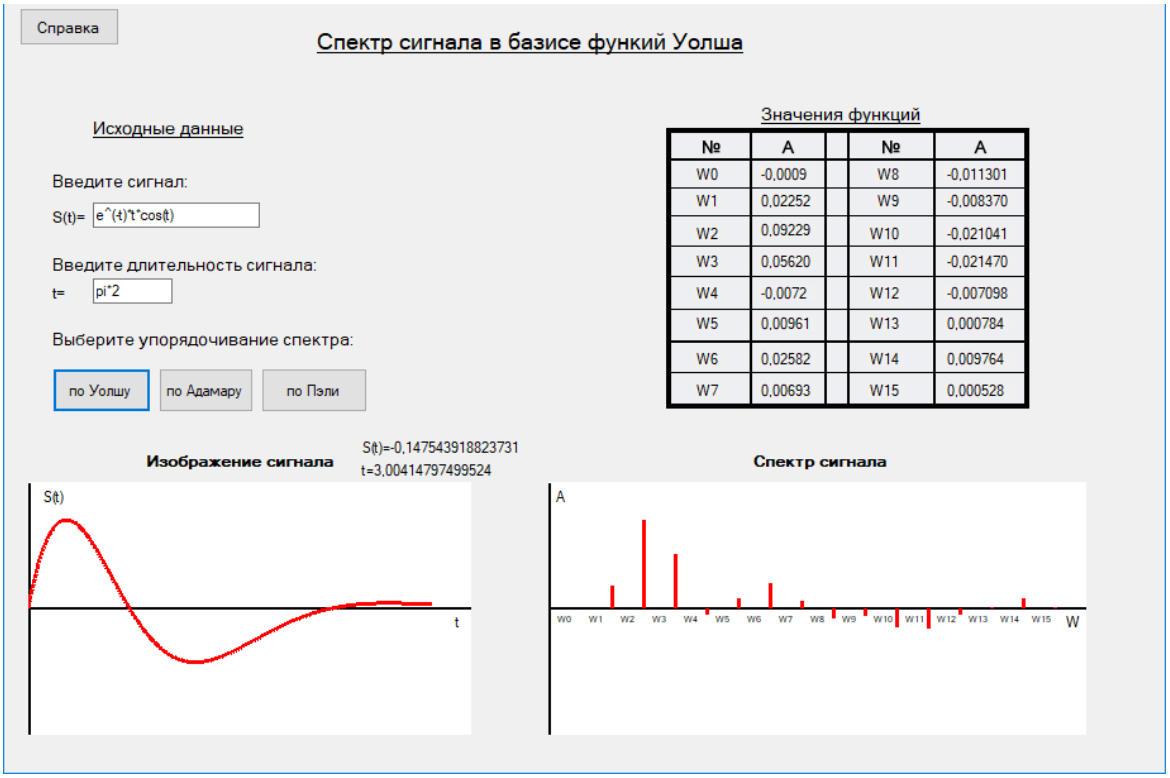


Рисунок 3 – Разложение функции e^(-t)*t*cos(t).

В результате исследования было установлено, что для разложения в базисе функций Уолша больше всего подходят периодические функции, т.к. количество нулевых спектральных составляющих меньше, чем при разложении непериодических функций.

Список используемых источников:

1. Гоноровский И.С. Радиотехнические цепи и сигналы. — М.: Радио и связь, 1986 г. – 512 с.