Министерство образования Республики Беларусь

Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 621.397.13 – 049.65

Рабцевич Виолетта Викторовна

# Технологии защиты телевизионной информации от несанкционированного использования

**АВТОРЕФЕРАТ**

на соискание степени магистра технических наук

по специальности 1-45 80 01 «Системы, сети и устройства телекоммуникаций»

Научный руководитель

Липкович Эдуард Борисович

доцент кафедры СТК

Минск 2016

# ВВЕДЕНИЕ. ПОСТАНОВКА ЗАДАЧИ

В настоящее время в сфере телекоммуникаций стал возможным массовый доступ к различным формам медиаконтента. Однако медиаконтент – это товар, который покупается и продается. Следовательно, он должен быть доступен только тем пользователям, которые за него платят, причем это важно не только для контент-провайдера, но и для обладателя прав на продукт.

Для защиты информации правообладателей могут применяться различные средства – в зависимости от оператора, который их выбирает, – но наиболее распространенными из них являются так называемые системы закрытия, или системы условного доступа. Без использования таких систем достаточно сложно предоставить абонентам платную форму услуг **с** авторизацией их доступа к теле- и радиопрограммам.

Многие из современных систем условного доступа берут свое начало еще в аналоговых спутниковых системах, в которых они выполняли исключительно роль защиты платных телеканалов от несанкционированного просмотра. В этих системах использовалась техника перемешивания строк передаваемого изображения по определенному алгоритму. Предполагалось, что только легальные приемники могут восстановить исходное изображение с помощью специального оборудования или программного обеспечения (ПО). Дальнейшее развитие СУД связано с использованием комбинации методов скремблирования и алгоритмов шифрования, что позволило значительно увеличить степень защиты телеканалов от нежелательного доступа.

В настоящее время на рынке цифрового вещания представлено достаточно большое число систем условного доступа. Среди них наибольшую популярность приобрели: DRECrypt, VideoGuardExpress, Verimatrix, Conax, Viaccess, Irdeto и др. Для большинства конечных пользователей цифровых телекоммуникационных систем СУД воплощаются или в виде смарт-карт, или в виде CAM-модулей, которые вставляются в соответствующий разъем интегрированного приемника-декодера (STB – *Set-Top-Box*) и позволяют пользователю получать доступ к различным информационным сервисам: телеканалам, радиоканалам, Интернет-ресурсам, телеконференциями многое другое.

Целью магистерской диссертации является рассмотрение технических решений и средств, предназначенных для защиты видеоинформации от несанкционированного просмотра, копирования и нелегального распространения.

Обобщены модули построения систем защиты видеоинформации при ее передаче по спутниковым и наземным каналам связи.

Вскрыты точки возможной утечки видеоинформации при ее передаче.

В процессе написания магистерской диссертации необходимо решить следующие задачи. Выполнить сопоставительный анализ современных и перспективных СУД, предназначенных для защиты контента при организации вещания по различным телекоммуникационным средам.

Выявить пути развития средств криптозащиты, обладающих повышенной устойчивостью к перехвату информации и нелегальному распространению материалов.

Разработать примеры построения систем вещания, в которых содержатся современные СУД. В частности, разработать структурные схемы и дать описание их функционирования.

Разработать структурные схемы передающих и приемных устройств системы условного доступа, а также дать описание их работы.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

В настоящее время в мире насчитывается более четырех миллиардов пользователей средств спутникового и наземного мультимедийного вещания и более двух миллиардов пользователей мобильных телефонов. Поэтому в большинстве современных разработок присутствуют решения по защите контента от несанкционированного использования, включая и защиту прав его правообладателей. Пропорционально росту количества потребителей возрастает потребность в защите информации от несанкционированного доступа. Выбор средств защиты контента продиктован типом коммерческой модели, способами доставки информации, характером самого контента, наличием возможности организовывать интерактивность в выбранной сети.

Для максимального контроля над использованием доставляемой информации предусматриваются различные технологии защиты услуг и контента.

На сегодняшний день закрытие информации в сфере цифрового теле- и радиовещания осуществляется на базе привнесения в цифровой сигнал искажений, до такого уровня, чтобы на приемной стороне без оплаченной карточки доступ был невозможен. Для этого в систему на стороне передачи вводится скремблирование и шифрованиеинформации, а для ее открытия на стороне приема - декодирование. Закрытие цифровой информации осуществляется либо на транспортном уровне, либо на уровне приложений. В большинстве решений используется принцип скремблирования сигналов на транспортном уровне.

В диссертационной работе излагаются основные положения по структуре построения систем условного доступа применительно к цифровым каналам спутникового и наземного телевещания. Приводятся теоретические положения по вопросам закрытия медиаконтента от несанкционированного просмотра, копирования и распространения.

В диссертационной работе ставятся и решаются следующие задачи:

– разработка структурных схем построения систем условного доступа для приемного и передающего спутникового оборудования;

– разработка структурных схем ограниченного доступа с обратным каналом при организации наземного цифрового вещания и кабельной доставки информации в формате IPTV;

– анализ способов маркирования контента и способов контроля над процессом передачи телеинформационных сигналов с обеспечением защиты от несанкционированного распространения.

– расчет системных показателей приемного оборудования;

## БАЗОВЫЕ ПОЛОЖЕНИЯ, ВЫНОСИМЫЕ НА ЗАЩИТУ

Во введении обосновывается актуальность выбранной темы, даётся краткая характеристика её разработанности, определяются объект и предмет исследования, цель и задачи, указана теоретико-методологическая основа, отмечены элементы научной новизны, формулируются основные положения диссертации, выносимые на защиту.

Первая глава «Сравнительный анализ технологий защиты информации в системах телекоммуникаций» включает общие положения по состоянию в области защиты контента и состоит из группы подразделов.

В подразделе 1.1. «Базовые положения по защите информации» производится общая классификация систем по основным признакам. Приводятся основные достоинства и недостатки различных способов построения.

В подразделе 1.2. «Способы реализации систем условного доступа» проводится сравнительный анализ карточного и бескарточного способа построения систем.

В подразделе 1.3. «Платформы системы условного доступа» рассмотрены наиболее известные способы кодирования, разработанные для применения в системах спутникового мультимедийного вещания..

В подразделе 1.5. «Алгоритм скремблирования для систем с ограниченным доступом» рассмотрены базовые положения единого алгоритма скремблирования цифрового потока.

Вторая глава «Устройства защиты информациииспутниковогоцифрового вещания» включает состав и структуру построения приемных и передающих устройств ограничения доступа при построении спутникового вещания..

В подразделе 2.1. «Структурная схема системы условного доступа» приводятся обобщенная структурная схема модели организации условного доступа для спутникового вещания.

В подразделе 2.2. «Передающая часть базовой системы условного доступа» приводится схема шифрования контента при передаче по спутниковой линии.

В подразделе 2.3. «Приемная часть системы условного доступа» приводится схема раскрытия шифрового контента при приеме.

В подразделе 2.4. «Демультиплексирование цифрового потока» рассмотрен процесс прочтения сервисной информации и анализа идентификаторов PID.

В подразделе 2.5. «Формирование сервисной информации в системах спутникового вещания» рассмотрены функции и структура сервисных таблиц.

В подразделе 2.6. «Структура построения передающего комплекса системы спутникового вещания» показано место системы условного доступа в схеме передающего комплекса ЦСВ.

Третья глава «Устройства защиты информации наземного цифрового вещания» состоит из трех подразделов, в которых рассматриваются вопросы построения систем условного доступа при организации наземного и IPTV телевидения.

В подразделе 3.1. «Структура системы условного доступа при организации вещания» представлена функциональная схема ограничения доступа в системе цифрового ТВ вещания.

В подразделе 3.2. «Головная станция системы MMDS» предложен вариант построения системы MMDS с обратным каналом.

В подразделе 3.3. «Структурная схема станции сопряжения сети IPTV» производится анализ возможных способов включения системы условного доступа при построении сетей IPTV.

Четвертая глава «Способы защиты информации от копирования и распространения» посвящена исследованию дополнительных сособов защиты авторских прав и контроля расспространения.

В подразделе 1.1. «Системы DRM» производится общая классификация систем по основным признакам..

В подразделе 1.2. «Маркирование телевизионных программ цифровыми водяными знаками» проводится.

Пятая глава «Расчет энергетических показателей на спутниковой радиолиинии исз – зс» включает вопросы снижения достоверности приема при наличии кратковременных помех и состоит из двух подразделов.

## ЗАКЛЮЧЕНИЕ

В процессе написания магистерской диссертации получены результаты, которые можно свести к следующему.

Представлен подробный обзор систем условного доступа про организации цифрового вещания. Из него следует, что система ограничения доступа является необходимым средством защиты контента от несанкционированного просмотра программ и нелегального копирования материала. Основы построения СУД распространяются как на системы спутникового вещания, так и на средства доставки программ по наземным и кабельным сетям.

Изложены принципы построения передающих и приемных устройств системы условного доступа с использованием специальных сообщений доступа (ECM и EMM) для декодирования зашифрованных программ.

Представлено большое число решений условного доступа при организации ТВ вещания по однонаправленным и интерактивным сетям. Во всех решениях используется принцип шифрования передаваемых ключей, аппаратные или программные средства дешифрации, карточные или бескарточные системы аутентификации пользователей и идентификации оплаченных программ или каналов.

Разработаны структурные схемы и дано описание работы при организации вещания по интерактивным сетям типа IPTV. Указана важность и целесообразность системы условного доступа в этих решениях.

Рассмотрен алгоритм прочтения сервисной информации необходимый для правильного демультиплексирования цифрового потока и декодирования закрытых программ на стороне пользователя.

Рассмотрены варианты борьбы с нелегальным копированием информации и ее распространением. Это методы водяных знаков и DRM. Благодаря совокупности принятых решений обеспечивается высокая криптографическая защита контента правообладателя.

По исходным данным, представленным в задании, произведен полный расчет энергетических и системных показателей на радиолинии.

Таким образом, рассмотрены все основные технические решения по созданию устройств защиты информации для различных сетей цифрового наземного и спутникового вещания.

## СПИСОК ОПУБЛИКОВАННЫХ РАБОТ АВТОРА

[А-1] Рабцевич, В.В. Центральная станция сопряжения интерактивной спутниковой сети/В.В. Рабцевич, Э.Б. Липкович, М.И. Зорько // Материалы. XX НТК – Минск : УО БГАС Современные средства связи. 14-15 октября 2015г, 2015. – 324с.(с.107)

[А-2] Рабцевич, В.В. Спутниковый интерактивный доступ к информационным ресурсам /В.В. Рабцевич, Э.Б. Липкович, Е.А. Костромин // Современные проблемы радиотехники и телекоммуникаций "РТ-2015": материалы 11-ой международной молодежной научно-технической конференции (Севастополь, 16-20 ноября 2015 г.) - Севастополь: СевГУ, 2015. - 255 с.(с.87)