УДК 338.47; 621.397.63

СИСТЕМА ОБЕСПЕЧЕНИЯ ЗАЩИТЫ УСЛУГ ЦИФРОВОГО ТЕЛЕВИДЕНИЯ

Сайдуллаев Умеджон Уктамович, *канд. экон. наук, доцент, заведующий кафедрой многоканальных телекоммуникационных систем ГОУ «ХГУ имени акад. Б. Гафурова» (Таджикистан, Худжанд)*

СИСТЕМАИ ТАЪМИНИ ҲИФЗИ ХИЗМАТРАСОНИҲОИ ТЕЛЕВИЗИОНИ РАҚАМӢ

Сайдуллоев Умедҷон Ӯктамович, *н.и.иқтисод., дотсент, мудири кафедраи системаҳои бисёршабакавии телекоммуникатсионии МДТ "ДДХ ба номи акад. Б. Ғафуров" (Тоҷикистон, Хуҷанд)*

THE SYSTEM OF PROVIDING PROTECTION RELATING TO THE SERVICES OF DIGITAL TV

Saidullaev Umedjon Uktamovich, *Candidate of Economic Sciences, Associate Professor, chief of the department of the department of multichanneled telecommunication systems SEI "KhSU named after acad. B. Gafurov" (Tajikistan, Khujand),*
E-mail: *saidullaev_umed@mail.ru*

Ключевые слова: *защита телевизионного контента, Интернет, цифровое телевидение, условный доступ, инновационные технологии, доход телевизионных компаний, предоставление услуг*

В статье обсуждается значимость и эффективность систем защиты услуг цифрового телевидения. Приведены некоторые результаты аналитического исследования современного состояния и перспектив развития цифровых технологий и защиты телевизионного контента. Рассмотрены тенденции развития монетизации цифрового телевизионного контента в Интернет-пространстве и их влияние на способы предоставления услуг цифрового телевидения. Изучены методы идентификации пользователей и контроля доступа к телевизионному контенту.

Вожаҳои калидӣ: *ҳифзи контенти телевизионӣ, Интернет, телевизиони рақамӣ, дастрасии шартӣ, технологияҳои инноватсионӣ, даромади ширкатҳои телевизионӣ, пешниҳоди хизматрасониҳо*

Дар мақола аҳамият ва самаранокии системаҳои муҳофизатӣ барои хизматрасониҳои телевизиони рақамӣ баррасӣ шудаанд. Баъзе натиҷаҳои таҳқиқоти таҳлилии вазъи кунунӣ ва дурнамои рушди технологияҳои рақамӣ ва ҳифзи контенти телевизионӣ оварда шудаанд. Тамоюлҳои рушди монетизатсияи контенти телевизиони рақамӣ дар фазои Интернет ва таъсири онҳо ба усулҳои пешниҳоди хизматрасониҳои телевизиони рақамӣ баррасӣ гардидаанд. Усулҳои мушаххаскунии истифодабарандагон ва назорати дастрасӣ ба контенти телевизионӣ омӯхта шудаанд.

Key words: *protection of TV content, Internet, digital TV, conditional access, innovational technologies, TV companies revenue, services rendering*

The article discusses the significance and effectiveness of the protection system related to rendering the services of digital TV. The author adduces certain results of analytical investigation of modern state and prospects of development of digital technologies and protection of telecontent. The author considers the tendencies of development of monetization of the digital content in the Internet space and their influence over the methods of digital TV services rendering. The methods of identification of users and access controlling television content have been studied.

Развитие телевидения напрямую связано с внедрением цифровых технологий, новых методов обработки и передачи сигнала, появлением каналов высокоскоростной связи. Внедрение цифровых технологий в сферу телевидения внесло колоссальные изменения в технологии передачи информации, расширило технологические возможности телевидения, способствовало появлению новых видов услуг и значительно расширило телевизионную аудиторию. Внедрение цифровых технологий позволило разработать новые модели телевизионного контента, улучшить качество предоставляемых услуг, расширить доступ пользователей к различным интерактивным формам коммуникации и многочисленным электронным сервисам.

Цифровые технологии изменили состав и спектр существующих методов реализации стратегии телевещания, а процесс телевещания в цифровом формате улучшил качество изображения и звука, возросла активность пользователей, увеличилась доходность, сократились издержки телекомпаний. Разработка телевизионного контента в цифровом формате, позволила усовершенствовать технологию редактирования и публикации телевизионных программ и методов её монетизации. Улучшения программного содержания, позволило телевидению расширить его аудиторию и произвести монетизацию телевизионного контента с максимальным охватом аудитории, что способствовало росту экономической эффективности предоставляемых услуг, повышению рентабельности работы телекомпаний.

Внедрение цифровых технологий обеспечило среду для интеграции телевидения с Интернетом, в результате которого изменилась культура потребления телевизионных продуктов, произошла трансформация телевизионной аудитории, появились новые виды услуг, увеличилось количество каналов и т. д. Интернет стал для телевидения дополнительной площадкой, которая позволила разместить телевизионный контент на разных интернет-порталах и максимально эффективно привлечь аудиторию [5, с.221]. Сегодня телевидение имеет собственные интернет – сервисы, где можно смотреть практически любые телевизионные каналы. Интернет - площадки предоставили телевидению возможность не только сохранить, но и увеличить аудиторию и произвести монетизацию. Расширение аудитории и её последующая монетизация позволили вещателям и создателям цифрового телевизионного контента получить высокий доход от его реализации на интернет - площадках.

Интернет-площадки обеспечили пользователям широкий доступ к различным сервисам, а это потребовало при выборе модели монетизации контента оценить его эффективность и убедиться в том, что он сможет принести доход вещателю и создателю цифрового контента. Выбор модели монетизации в данном случае является одним из ключевых моментов, от которой зависит стратегия маркетинга и другие важнейшие параметры монетизации. В настоящее время монетизация телевизионного контента в основном производится по двум моделям - подписке и абонентской плате, которые являются самыми популярными моделями и ими пользуется большинство вещателей. Монетизация телевизионного контента - это метод, с помощью которого телекомпания получает доход от распространения телевизионного продукта.

Расширение аудитории является важной частью стратегии маркетинга телекомпании, направленного на максимальное распространение контента и сложения целевой аудитории с использованием различных каналов и платформ. Как показывает опыт, активное размещение на онлайн-площадках большинства телеканалов является одним из методов монетизации контента, расширения аудитории и увеличения доходов телекомпании. Онлайн - площадки телеканалов позволяют потребителям удовлетворять их потребности благодаря огромному количеству новостных и развлекательных каналов с хорошим качеством звука и изображения. Стоит отметить, что телеканалы предлагают актуальный контент на своих платформах ещё до его показа, используя платную модель монетизации по подписке. Это сделано для того, чтобы побудить лояльных потребителей контента подписаться на него и привлечь внимание новых потребителей с целью увеличения аудитории.

Разработка содержательного и актуального цифрового телевизионного контента и его монетизация с последующим вещанием на различных онлайн-площадках требует улучшения его защиты от несанкционированного доступа. В нынешних реалиях доступ потребителей к вещательной системе осуществляется за счёт специального подключения к вещательной системе, а также за счёт специального протокола доступа, где возможность для просмотра программы обусловлена оплатой услуг. Требования к надёжности системы защиты цифрового телевизионного контента возрастают из-за круглосуточного режима работы, безотказности и высокой устойчивости всех узлов к предельным нагрузкам сети, перепадам напряжения и температурного режима. Важным критерием при оценке надёжности системы защиты телевизионного контента является быстрота действий и высокая производительность. Экономическое благосостояние телевещательной компании напрямую зависит от надёжности систем защиты, так как в случае взлома системы и утечки ключей доступа или незаконного копирования и распространения контента экономический ущерб будет значительным. Перманентный мониторинг корректности работы системы защиты позволит своевременно обнаружить и блокировать утечку важной информации.

Несанкционированный доступ, взлом, пиратство приводят к уменьшению прибыли телекомпаний, потере важной информации или к полной блокировке системы и повреждению файлов. Для предотвращения подобных рисков, связанных с нарушениями безопасности

системы защиты, необходимо обеспечить защиту от потери данных из-за неисправности программного обеспечения, ошибок технического персонала и пользователей сетевых ресурсов и принять соответствующие меры для бесперебойной работы системного оборудования. Надёжная работа системы защиты телевизионного контента позволяет телекомпании увеличит доход от реализации телепродукта путем монетизации, сохранить критически важную информацию и обеспечить защиту авторских прав.

Для обеспечения эффективной защиты телевизионного контента от несанкционированного доступа используются высокотехнологичные устройства и современное программное обеспечение. Любая телекомпания имеет оригинальный контент, критически важную информацию, которая нуждается в защите от желающих получить к ней доступ. Для этого существует много средств защиты телевизионного контента от несанкционированного доступа на примере систем SIEM (Система управления информационной безопасностью и событиями безопасности), которые способны оперативно обнаружить внешние и внутренние атаки, распознавать, анализировать и оценивать уровень защиты. «Защиту от несанкционированного доступа к телевизионному контенту можно обеспечить методами защиты систем SIEM, системой учётных записей и паролей, мониторингом и протоколированием, механизмами управления доступом и специализированными программно–техническими комплексами защиты данных» [6, с.484].

Системы защиты телевизионного контента от несанкционированного доступа позволяют операторам контролировать доступ незарегистрированных пользователей к определённому контенту и своевременно их заблокировать. Но не смотря на существующие системы защиты от негативных внешних воздействий, в последние годы преступность в этой сфере не только увеличивается, но и совершенствуется технически и технологически. Это связано прежде всего с научно-техническим прогрессом, эволюцией информационных технологий и формированием новой среды, использующей современные инновационные технологии. Поэтому новая среда, использующая современные инновационные технологии, порождает преступные группы, отдельных злоумышленников, пиратов и другие сообщества, способные нарушить штатную работу каналов связи и системы передачи информации, осуществить взлом системы защиты, копирование и несанкционированный доступ к телевизионному контенту.

Это обстоятельство требует совершенствования системы защиты телевизионного контента от негативных внешних воздействий, направленных на незаконное вторжение. Незаконное вторжение, или несанкционированный доступ - это противоправное преднамеренное овладение или копирование телевизионным контентом лицом, которое не имеет права доступа к нему. Другими словами, это незаконное овладение телевизионным контентом с целью его копирования и дальнейшей реализации по умеренно низкой цене для получения дохода. В любом случае при незаконном доступе к телевизионному контенту нарушаются авторские права, проблема решается в судебном порядке.

Поэтому система защиты от незаконного доступа должна работать безотказно и объединять все уровни защиты телевизионного контента. Только при наличии всех элементов защиты телевизионного контента, работающих в едином ритме, достигается эффективность работы системы защиты, которая способна предотвращать любые атаки и надёжно защитить от негативных внешних воздействий, направленных на незаконное вторжение.

Незаконный доступ к телевизионному контенту может быть реализован по разным сценариям и с использованием разных методов. Каждый несанкционированный доступ к телевизионному контенту - это не только потеря прибыли, но и ощутимые материальные потери для телекомпании. Не случайно незаконный доступ к телевизионному контенту сегодня становится одной из самых острых проблем, которая ежегодно приносит телекомпаниям огромный экономический урон.

Для решения данной проблемы проводится огромная работа по совершенствованию системы защиты телевизионного контента, в частности разрабатываются сложные структуры защиты, которые позволяют авторизовать доступ пользователей к контенту; используются системы и устройства для защиты телевизионного контента, которые могут ограничить или полностью запретить доступ к нему злоумышленников, системы обнаружения и предотвращения вторжений, межсетевые экраны. Кроме того, сегодня созданы эффективные многофункциональные системы защиты телевизионного контента от несанкционированного доступа и копирования с хорошими эксплуатационными характеристиками, обеспечивающие устойчивость к взлому.

Одной из таких систем является система условного доступа CAS (Conditional Access System). Система CAS является комплексом программных и аппаратных устройств, позволяющих доступ к кодированным каналам. Система условного доступа обладает большой гибкостью. Уровень защиты системы CAS позволяет надёжно защитить телевизионный контент от несанкционированного доступа и обеспечивает доступ только для авторизованных подписчиков.

Результаты исследований учёных Н.В. Лысенко и Г.М. Лабкова можно применить на практике: «Указанный принцип выбора контейнеров позволяет повысить устойчивость алгоритма к несанкционированному доступу, поскольку максимально на одном изображении изменяется лишь один пиксель. Исследованный алгоритм Куттера–Джордана–Боссена способен работать в режиме реального времени как для внесения скрытой информации в видеопоток, так и для её извлечения» [3, с.46]. Ещё одной надёжной системой защиты телевизионного контента является метод криптографии.

Криптографические методы шифрования ключей доступа к сетевым ресурсам телевещательных компаний стали использоваться относительно недавно. Доступ к телевизионным платным каналам защищается с целью взимания абонентской платы за просмотр.

В целях повышения эффективности кодирования операторами спутникового, а также наземного вещания перманентно усложняются и совершенствуются методы шифрования ключей доступа к ресурсам телевещательных сетей. Существуют две схемы шифрования: симметричная и асимметричная. Обе схемы шифрования могут значительно снизить риск утечки и разглашения информации и являются простыми, доступными и экономически выгодными средствами защиты для телекомпании. «Как известно, степень безопасности алгоритма зависит от сложности алгоритмов шифрования и длины ключа. Разработанная российскими учёными система условного доступа "Роскрипт-М" использует 8 уровней защиты (пароли, базовые ключи, имитовставки и т.д.)» [2, с.216].

Таким образом, телекомпании, которые смогли обеспечить высокий уровень защиты телевизионного контента, могут оградиться от всевозможных атак и взломов, что будет способствовать росту конкурентоспособности и увеличению доходов телекомпании от монетизации.

В нынешних условиях, чтобы избежать негативных внешних воздействий, направленных на незаконное овладение телевизионным контентом и нарушение состояния защиты информации, необходимо использовать программные пакеты, позволяющие заблокировать доступ к информации. По мнению учёного В.В. Мкртичяна, специализирующегося на защите информации в вещательных сетях, с помощью создания аппаратно-программной модели с эффективной схемой специального широковещательного шифрования можно «…гарантированно находить как минимум, одного, а иногда и всех членов коалиции злоумышленников, атакующих систему защиты, в случае, когда мощность коалиции не превышает некоторого заранее предусмотренного в системе порога» [4, с.204].

Это лучший способ защиты информации от незаконного вторжения или взлома системы. Однако взлом может происходить в момент проявления уязвимости системы защиты, и в этот момент защищённые файлы могут быть перехвачены злоумышленниками.

Поэтому важно вовремя выявлять недостатки в работе установленных программных и аппаратных компонентов. Также потеря критически важной информации может происходить по вине сотрудников телекомпании, что может нанести больший ущерб, чем сбой всей системы. Для устранения таких потерь принимаются меры, ограничивающие доступ персонала к критически важной информации, путём разработки правил, ограничивающих права лиц, не имеющих доступа к конфиденциальной информации. В них предусматриваются действия сотрудника, имеющего доступ, таким образом, что он может использовать только данные, которые нужны для его работы. И другие сотрудники работают только с теми данными, которые нужны им для работы. Таким образом, принятые меры не дают сотрудникам возможность иметь полную картину по важной критической информации, необходимой для злоумышленников.

Обеспечение телевизионного контента надёжной системой защиты от копирования способствует выстраиванию разумных отношений между участниками процесса по купле и продаже контента и рекламы на телевидении. Отсутствие должной системы защиты может привести к незаконному доступу и возможности произвести копирование телевизионного контента с целью дальнейшего показа на других онлайн – площадках. Незаконно

скопированный телевизионный контент обычно реализуется по умеренно низким ценам, что приводит к потере немалой части дохода правообладателями контента. Проблема пиратства, или незаконного показ контента, на который у компании нет прав, возникла давно и по сей день используется недобросовестными операторами.

Сегодня пиратство приносит большой доход от незаконных действий, копирование фильмов или сериалов и размещение их в YouTube, в «Одноклассниках» и на других Интернет-ресурсах приносит финансовые потери правообладателям.

Поэтому телевизионные компании и правообладатели телевизионного контента недовольны большими потерями доходов из-за нарушения авторских прав. Обнаружить нарушителей авторских прав, копирующих контент, в нынешних условиях очень сложно, т.к. они в своей деятельности применяют всё более сложные современные технологии копирования.

Для защиты авторских прав разработана система защиты DRM (Digital Rights Management) - «система управления цифровыми правами». DRM защищает телевизионный контент от незаконного копирования и просмотра. DRM - системы используют технологию скремблирования и шифрования в различных вещательных сетях. Телевизионным контентом, защищённым CAS и DRM-системами, потребитель сможет воспользоваться в том случае, если его телевизионная приставка имеет чип дешифрации. Таким образом, системы защиты CAS и DRM способны защитить критически важную информацию, телевизионный контент и авторские права. Исследователи П.В. Ересько и В.И. Гудаева утверждают: «К техническим средствам защиты авторских прав относят любые цифры и коды, в которых содержится информация, идентифицирующая произведение автора, либо информация об условиях использования произведения, которая содержится на оригинале или экземпляре произведения, приложена к нему или появляется в связи с сообщением в эфир или по кабелю» [1, с.135]. Эти системы позволяют операторам контролировать процесс распространения контента и производить монетизацию своих услуг.

В последнее время, несмотря на принятые меры по снижению абонентской платы, телекомпаниям не удаётся расширить аудиторию и увеличить доход от монетизации телевизионного контента. Это связано прежде всего с нарушением авторских прав, поскольку телекомпаниям приходится конкурировать с нелицензированными OTT- платформами и другими недобросовестными операторами, злоумышленниками, копирующими телевизионный контент с целью получения дохода. Уменьшение доходов телекомпаний снижает дальнейший рост их экономических показателей.

Одним из наиболее эффективных методов защиты авторских прав является патентирование интеллектуальной собственности или получение лицензии, которые подтверждают наличие прав на авторство. Кроме того, сегодня существует достаточное количество различных инструментов для защиты авторских прав, которые охраняются законом. Однако, несмотря на все существующие механизмы защиты, происходят случаи нарушения авторских прав. Механизм защиты авторских прав осуществляется в административном и судебном порядке. Разработка оригинального телевизионного контента все чаще становится предметом дискуссий, когда авторы не смогли своевременно оформить права на авторство.

Развитие инновационных технологий привело к совершенствованию системы защиты и ограничению доступа к услугам цифрового телевидения. В такой системе защиты телекомпании повсеместно используют систему условного доступа с программно- аппаратным решением, которое способно надёжно защитить телевизионный контент от несанкционированного доступа. Распространена практика коллективного использования незаконно добытой смарт-карты при помощи шаринга, т.е. подключения к удалённым оригинальным смарт-картам, которые находятся на сервере, через сеть Интернет. В последние годы злоумышленники стали использовать изощрённые методы взлома, при помощи которых они могут преодолеть защитные барьеры системы доступа. Для злоумышленников ценность телевизионного контента имеет большое значение, поэтому они представляют большую опасность и приносят большой урон телекомпаниям по сравнению с другими видами взлома. Пиратский взлом бывает двух видов:

1. непрофессиональный;
2. профессиональный.

Непрофессиональные пираты используют разные методы взлома для интереса, и это для них просто развлечение. Профессиональные пираты - это серьёзные преступные сообщества, имеющие большой опыт и соответствующий капитал, при помощи которых они могут нанести огромный экономический ущерб телекомпаниям.

Современные системы защиты телевизионного контента от несанкционированного доступа разработаны на основе аппаратных решений и имеют надёжную систему устойчивости к взлому. Телевизионный контент шифруется с помощи ключа, методом криптографии и скремблирования. Объектом атаки могут стать STB и модули доступа (CAM). Они считаются открытыми системами, поэтому являются самым слабым звеном в цепи. Степень риска от атаки можно уменьшить за счёт ограничения доступа к открытым ресиверам, что повысит степень защищённости доступа.

Сегодня системы защиты телевизионного контента от несанкционированного доступа демонстрируют эффективные способы борьбы с «шарингом». Внедрение комплексной системы защиты от «шаринга» требует её работы независимо от систем условного доступа. Поэтому сегодня многие производители систем условного доступа разрабатывают системы защиты ресивера отдельно от системы условного доступа. Такие системы надёжно защищают от «шаринга» и не позволяют нанести ущерб телекомпаниям, сохраняя их доходы. Кроме шаринга, существует кардшаринг, задача которого - раскодирование платных каналов. По одной оплаченной карте множество абонентов может получить доступ к закрытым каналам. Такой способ позволяет уменьшить размер абонентской платы. Однако некоторые пользователи ради экономии денег пользуются пиратскими смарт-картами, которые очень популярны у пользователей телевизионного контента.

Кардшаринг - это продажа оплаченной смарт-карты, позволяющей осуществить общий доступ к платным закодированным сервисам за гораздо меньшую плату. Приобретение такой смарт-карты позволяет получить полный доступ к множеству пакетов, каждый из которых содержит сотни каналов. Необходимо отметить, что разработчики систем условного доступа постоянно совершенствуют методы борьбы с шарингом, однако пока существенных успехов это не приносит. Кроме того, с целью защиты от шаринга, операторы часто меняют ключи, которые декодируют телевизионный сигнал каждые 5-10 секунд.

Таким образом, можно заключить, что операторам необходимо создать ассоциацию телевещательных операторов с целью защиты интересов и борьбы с несанкционированным доступом к телевещательной сети. Ассоциации необходимо вести мониторинг телевещательного рынка с целью выявления несанкционированных подключений, определения серверов кардшаринга по IP-адресам, выяснения (совместно с правоохранительными органами) лиц, организовавших кардшаринг, и привлечения их к ответственности.

ЛИТЕРАТУРА:

1. Ересько П.В.Защита авторских прав в сети интернет / П.В. Ересько, В.И. Гудаева // Приоритетные научные направления: от теории к практике. 2016. №25-1. С. 133-138.
2. Ляшко А.А.Система условного доступа "Роскрипт-М". Область применения. Параметры / А.А. Ляшко, И.В. Кононенко // T-Comm: Телекоммуникации и Транспорт. 2009. №S1. С. 216-219.
3. Лысенко Н.В.Применение стеганографического алгоритма Куттера-Джордана-Боссена в видеопоследовательностях / Н.В. Лысенко, Г.М. Лабков // Известия вузов России. Радиоэлектроника. 2015, №4. - С. 44-46.
4. Мкртичян, В.В. Об экспериментальном исследовании надёжности и применении схемы специального широковещательного шифрования/В.В.Мкртичян// Известия Южного Федерального Университета. Технические науки. 2008, №8. - С. 203—210.
5. Сайдуллаев, У.У. Эффективность организации условного доступа в сетях телевизионного вещания Республики Таджикистан / У.У. Сайдуллаев // «Вестник университета». РТСУ, Душанбе, 2018, №3. - С. 221—229.
6. Федотов, В.Х. Защита от несанкционированного доступа и экономическая эффективность информационных систем / В.Х. Федотов // Вестник Чувашского университета. – 2007, № 4. – С. 483-493.

REFERENCES:

1. Eresko P.V., Gudaeva V.I. Copyright protection on the Internet / P.V. Eresko, V.I. Gudaeva // Priority scientific directions: from theory to practice. 2016. № 25-1. P.133-138.
2. Lyashko A.A., Kononenko I.V. Conditional access system "Roskript-M". Application area. Parameters / A.A. Lyashko, I.V. Kononenko // T-Comm: Telecommunications and Transport. 2009. №1. P.216-219.

3. Lysenko N.V., Labkov G.M. Application of Stenographical Algorithm of Cutter- Jordan – Bassen in Video successions / N.V. Lysenko, Y.M. Labkov // Tidings of Russia Higher School. Radioelectronics. 2015. № 4. P. 44-46.
4. Mkrtichyan V.V. On Experimental Research of Reliability and application of the scheme of special Broad Casting Cyphering // V.V. Mkrtichyan // Tidings of the South Federal University. Technical Sciences. 2008. №8 P. 203-210.
5. Saidullaev U.U. Effectivity of Organization of Conventional Access in the networks of Tajikistan Republic Telecasting / U.U. Saidullaev // RTS Bulletin. Dushanbe. 2018. №03. P.221-229.
6. Fedotov V.Kh. Protection from non-Sanctioned Access and Economic Effect of Informational Systems / V. Kh. Fedotov // Bulletin of Chuvash University. 2007. №04. P.483-493.