Микулин Ю.С. Эволюция технологий защиты от пиратства в играх: от классических методов до новейших решений // Международный журнал информационных технологий и энергоэффективности. – 2024. –
Т. 9 № 2(40) с. 11–20

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ЭВОЛЮЦИЯ ТЕХНОЛОГИЙ ЗАЩИТЫ ОТ ПИРАТСТВА В ИГРАХ: ОТ КЛАССИЧЕСКИХ МЕТОДОВ ДО НОВЕЙШИХ РЕШЕНИЙ

Микулин Ю.С.
ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА", Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков д.22, корп.1), e-mail: ho11owabyss45@gmail.com

В данной статье исследована эволюция технологий защиты от пиратства в компьютерных играх, подразумевая обзор исторического развития защиты, начиная от первых методов, таких как CD-ключи, до современных решений DRM (Digital Rights Management) и новейших инноваций. В работе рассматриваются классические приемы защиты, их недостатки и анализируются современные тенденции, вызовы и угрозы пиратства в игровой индустрии.

Ключевые слова: Информационная безопасность, программное обеспечение в сфере ИБ, защита от нелегального копирования, DRM (Digital Rights Management), информационной технологии.

THE EVOLUTION OF ANTI-PIRACY TECHNOLOGIES IN GAMES: FROM CLASSICAL METHODS TO THE LATEST SOLUTIONS

Mikulin Y.S.
BONCH-BRUEVICH ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS, St. Petersburg, *Russia (193232, St. Petersburg, 22 Bolshevikov Ave., bldg. 1), e-mail:* ho11owabyss45@gmail.com

The article explores the evolution of anti-piracy technologies in computer games, providing an overview of the historical development of protection methods from early approaches like CD keys to modern DRM (Digital Rights Management) solutions and the latest innovations. It examines classical protection techniques, their limitations, and analyzes current trends, challenges, and threats posed by piracy in the gaming industry.

Keywords: Information security, software in the field of information security, protection against illegal copying, DRM (Digital Rights Management), information technologies.

Современная игровая индустрия представляет собой динамичный и конкурентоспособный рынок, где разработчики стремятся создавать увлекательные игровые продукты, вдохновляющие и привлекающие широкую аудиторию. Однако, наряду с ростом популярности и доступности игр, несанкционированное распространение и нелегальное копирование игрового контента стали серьезными проблемами, угрожающими доходам разработчиков и издателей, а также влияющими на целостность и безопасность игровой индустрии в целом. Исторически, защита от пиратства в играх эволюционировала от простых методов, таких как использование CD-ключей, до более сложных систем DRM (Digital Rights

Management) и других инновационных технологий, разработанных для предотвращения нелегального копирования и использования игрового контента. В настоящее время, в условиях быстрого развития технологий, вопрос защиты от пиратства остается актуальным, требуя постоянного совершенствования и адаптации к изменяющимся угрозам[2].

Исторический обзор защиты от пиратства в играх:

Ранние методы защиты от пиратства в компьютерных играх были основаны на простых, но в то же время эффективных техниках. Вот несколько ранних методов защиты и их эволюция:

1. CD-ключи (CD keys):

Ранние методы: Игры поставлялись с уникальным серийным номером, который требовался для установки и запуска игры.

Эволюция: Эти ключи начали использоваться широко в 1990-х, но с развитием интернета и возможности онлайн-активации, такие методы стали менее эффективными из-за легкости их подделки.

2. Физические защитные элементы:

Ранние методы: Некоторые игры включали физические элементы защиты, такие как флоппи-диски с защитными данными или дополнительные устройства (dongles), которые требовались для запуска игры.

Эволюция: Такие методы, хотя и обеспечивали высокий уровень защиты, стали неудобными для пользователей, так как требовали дополнительного оборудования или уязвимы к физическим повреждениям.

3. Защита от копирования (Copy protection):

Ранние методы: Эти методы включали в себя использование специальных программ или кодирования на физических носителях, что делало копирование и распространение сложным или невозможным.

Эволюция: С развитием технологий, такие защиты стали преодолеваться и обходиться, используя методы обхода или кряки.

4. Обнаружение изменений (Tamper detection):

Ранние методы: Это включало в себя проверку целостности файлов игры для обнаружения изменений или подделок.

Эволюция: Методы обхода и внедрения в файлы для изменения кода позволили пиратам преодолеть эти защиты.

5. Шифрование (Encryption):

Ранние методы: Использование шифрования данных игры для предотвращения нелегального доступа и чтения данных.

Эволюция: Шифрование продолжает развиваться, но с развитием методов обхода и взлома, требуются более совершенные алгоритмы.

Эти ранние методы защиты постоянно эволюционировали в ответ на новые вызовы, но также и пиратские методы обхода защиты, создавая постоянный баланс между защитой игр и удобством пользователей.

Преимущества и недостатки классических методов защиты:

Классические приёмы защиты в компьютерных играх имеют как преимущества, так и недостатки, которые важно учитывать:

Преимущества классических приёмов защиты:

1. *Отталкивание от неопытных пользователей*: Некоторые методы защиты, такие как CD-ключи или физические защитные элементы, создавали преграду для менее опытных пользователей, затрудняя пиратство из-за отсутствия знаний о способах обхода защиты.
2. *Дополнительные сложности для пиратов*: Многие из этих методов создавали дополнительные сложности для пиратов, что замедляло процесс взлома и требовало больше времени и усилий для обхода защиты.
3. *Уровень общей безопасности*: В свое время, такие методы как физические защитные элементы предоставляли более высокий уровень безопасности, чем некоторые современные электронные системы защиты.

Недостатки классических приёмов защиты:

1. *Неудобство для пользователей*: Многие из ранних методов защиты могли быть неудобными для пользователей, требуя наличие дополнительного оборудования или специальных условий для запуска игры.
2. *Ограниченность эффективности*: С развитием интернета и технологий, многие классические методы защиты стали менее эффективными из-за легкости обхода или подделки.
3. *Потенциальные угрозы* безопасности: Некоторые методы защиты, такие как использование физических защитных элементов, могли создавать потенциальные угрозы безопасности, например, если устройство было повреждено или утеряно.
4. *Ограничение продаж и распространения*: Некоторые методы защиты могли ограничивать продажи и распространение игр, так как требовали наличие дополнительных ключей или элементов для доступа к контенту.

Современные вызовы и угрозы пиратства в игровой индустрии:

Современные угрозы и тенденции в сфере пиратства в играх постоянно меняются и развиваются, оказывая влияние на безопасность игровой индустрии[1]. Ниже приведены основные угрозы и тенденции, которые в настоящее время актуальны:

1. *Онлайн-пиратство и дистрибуция через торренты*: Онлайн-кряки и пиратские сайты для скачивания игр становятся все более распространенными. Пираты создают копии игровых файлов и делятся ими через торрент-сети, обходя официальные магазины и магазины приложений.
2. *Социальное пиратство и обмен контентом*: Пиратство стало частью обмена контентом в социальных сетях, форумах и сообществах игроков. Читы, кряки и нелицензионный контент активно обсуждаются и распространяются среди пользователей.
3. *Развитие технологий взлома и обхода защиты*: Постоянно улучшающиеся методы взлома и обхода защиты позволяют пиратам обходить существующие механизмы защиты, открывая доступ к игровым материалам и функциям.
4. *Модификации и читы в мультиплеерных играх*: В мультиплеерных играх пираты могут использовать модификации или читы, которые дают преимущество над другими игроками, что нарушает баланс игрового процесса.

5. *Влияние на индустрию и разработчиков*: Пиратство снижает доходы компаний-разработчиков и издателей, что может привести к сокращению инвестиций в новые проекты и снижению качества игр.

6. *Угрозы безопасности и мошенничество*: Некоторые пиратские сайты могут быть источником вредоносного программного обеспечения и мошенничества, предлагая скачивание игр вместе с вирусами или троянскими программами.

7. *Мобильное пиратство*: С развитием мобильных игр и приложений, появляются новые методы пиратства и обхода защиты в мобильной индустрии.

Эти угрозы и тенденции вызывают кучу проблем, вот пример основных:

1. *Финансовые потери для разработчиков и издателей***:** Пиратство ведет к финансовым убыткам для компаний-разработчиков и издателей, так как пираты получают доступ к игровому контенту без оплаты, не принося доход компаниям за их труд и творчество[4].

2. *Ущерб для инноваций и новых проектов***:** Убытки от пиратства могут негативно повлиять на способность компаний-разработчиков вкладывать средства в новые и инновационные проекты, что может замедлить развитие игровой индустрии.

3. *Искажение данных о продажах***:** Некоторые данные о продажах игр могут быть искажены из-за наличия пиратских копий, что делает сложным оценку реального успеха игры и может повлиять на стратегию маркетинга.

4. *Угрозы для целостности и качества контента***:** Пираты могут модифицировать игровой контент, добавлять вредоносное программное обеспечение или изменять код игры, что угрожает ее целостности и качеству.

5. *Отрицательное влияние на игровое сообщество***:** Пиратство может создавать дисбаланс в онлайн-играх из-за использования читов и модификаций, что негативно сказывается на игровом опыте для честных игроков[1].

6. *Потенциальные риски для безопасности и конфиденциальности***:** Скачивание пиратского контента с ненадежных источников может представлять риски для безопасности пользовательского устройства из-за вирусов и вредоносных программ[5].

Эти проблемы, связанные с нелегальным копированием игрового контента, создают серьезные вызовы для игровой индустрии и требуют разработки и внедрения более эффективных методов защиты и борьбы с пиратством.

Современные технологии и методы защиты:

Существует несколько современных технологий и методов защиты от пиратства в играх, каждый из которых имеет свои преимущества и недостатки. Ниже приведен обзор некоторых из них:

1. Denuvo — это одна из наиболее известных и широко используемых технологий защиты от пиратства в игровой индустрии. Она разработана компанией Denuvo Software Solutions GmbH и представляет собой антипиратскую технологию, использующую множество механизмов для защиты игрового контента от несанкционированного доступа и копирования.

Ключевые особенности и характеристики Denuvo:

- *Асимметричное шифрование***:** Denuvo использует асимметричное шифрование для защиты цифровых подписей и ключей, связанных с лицензированием игр.
- *Анти-тампер защита:* Один из основных элементов Denuvo - это механизм анти-тампер защиты, который пытается предотвратить изменения в исполняемых файлах игры, делая их сложными для взлома и модификации.
- *Лицензирование в реальном времени:* Технология требует постоянной связи с серверами Denuvo для проверки лицензии, что делает сложным использование пиратского контента без активной и подлинной лицензии.
- *Обновления защиты:* Denuvo периодически обновляется, чтобы противостоять новым методам взлома и обхода защиты. Обновления встраиваются в патчи игр для повышения уровня защиты.
- *Многоплатформенность:* Технология Denuvo предназначена для различных игровых платформ, включая ПК, консоли и мобильные устройства.
- *Критики и контроверсии***:** Несмотря на широкое использование, Denuvo также сталкивается с критикой. Некоторые игроки высказывают опасения относительно влияния технологии на производительность игры и возможное увеличение нагрузки на процессор.

Несмотря на обширное использование, некоторые группы хакеров все же смогли обойти защиту Denuvo в некоторых играх, однако новые версии и обновления технологии постоянно внедряются для повышения эффективности защиты и обеспечения безопасности игрового контента.

2. Steam DRM - это технология цифрового управления правами, которая используется в платформе цифровой дистрибуции игр Steam, созданной компанией Valve Corporation. Она предназначена для защиты игрового контента, приобретаемого и запускаемого через платформу Steam.

Ключевые особенности и характеристики Steam DRM:

- *Лицензирование игр***:** Steam DRM используется для лицензирования игр, приобретенных через Steam. Пользователи получают доступ к своим играм через свою учетную запись Steam, что ограничивает возможность использования игр на нескольких устройствах без необходимости повторной покупки.
- *Автоматические обновления и патчи:* Один из преимуществ Steam DRM - это автоматические обновления и патчи для игр. Это позволяет разработчикам оперативно выпускать исправления ошибок и обновления безопасности.
- *Защита от несанкционированного доступа:* Steam DRM обеспечивает защиту от несанкционированного доступа к играм. Игры, купленные через Steam, требуют активацию через платформу и часто связываются с учетной записью пользователя, что делает сложным использование пиратского контента.
- *Ограничения для пользователей***:** Некоторые аспекты Steam DRM могут ограничивать возможности пользователей, такие как ограничения на одновременное использование игр на нескольких устройствах или требования постоянного подключения к интернету для проверки лицензии.
- *Поддержка разных платформ:* Steam DRM обеспечивает поддержку не только на PC, но и на других платформах, таких как Mac и Linux.

- *Подверженность взлому:* Как и другие системы DRM, Steam DRM также подвержен взлому и обходу, что позволяет пользователям создавать пиратские копии игр.

3. Античиты (Anti-Cheat) представляют собой программные инструменты, реализованные в играх для обнаружения и предотвращения использования читов, взломов или других нечестных методов игры, которые дают игрокам несправедливое преимущество или нарушают правила игры. Они играют ключевую роль в поддержании честной игровой среды в многопользовательских онлайн-играх.

Ключевые аспекты античитов:

- *Методы обнаружения:*

А) Мониторинг памяти: Античиты могут контролировать и анализировать память игрового процесса для обнаружения изменений, связанных с читами или взломом.

Б) Мониторинг сетевой активности: Они могут следить за сетевыми операциями игрока, чтобы выявить подозрительное поведение, такое как скорректированные данные, чрезмерное движение, и т.д.

В) Сравнение с паттернами: Античиты могут сравнивать поведение игрока с предопределенными паттернами, чтобы выявить аномалии.

- *Методы предотвращения:*

А) Блокировка доступа: Античиты могут блокировать доступ к игровым серверам для игроков, обнаруженных при использовании читов.

Б) Бан аккаунта: При обнаружении читов или взломов античит может накладывать временный или постоянный бан на аккаунт игрока.

- *Популярные античиты:*

А) Valve Anti-Cheat (VAC): Используется в играх на платформе Steam для обнаружения читерства и взломов.

Б) BattlEye: Часто применяется в многопользовательских онлайн-играх, таких как ARMA, PUBG, Rainbow Six Siege и др.

В) Easy Anti-Cheat (EAC): Используется в различных играх для обеспечения честной игровой среды.

4. Защита облачных серверов - это совокупность мер и технологий, направленных на обеспечение безопасности данных, хранимых и обрабатываемых в облачных вычислениях. Облачные серверы предоставляют ресурсы для хранения данных и выполнения вычислительных задач через интернет, и их безопасность является критически важной.

Ключевые аспекты защиты облачных серверов:

- *Шифрование данных:* Данные, хранящиеся на облачных серверах, часто шифруются. Это может включать шифрование в покое (данные в хранении) и шифрование в движении (данные, передаваемые между серверами и устройствами).
- *Механизмы аутентификации и авторизации:* Облачные сервера используют механизмы аутентификации, такие как многофакторная аутентификация (MFA), чтобы проверить легитимность пользователей. Они также предоставляют уровни авторизации для различных уровней доступа к данным.

- *Физическая безопасность:* Центры обработки данных (ЦОДы), где хранятся облачные серверы, обычно защищены физически: доступ ограничен, есть системы видеонаблюдения, биометрические системы и другие меры безопасности.
- *Мониторинг и обнаружение угроз:* Облачные провайдеры обычно используют системы мониторинга и обнаружения угроз (IDS/IPS), которые анализируют трафик данных для выявления аномалий или потенциальных атак.
- *Регулярные обновления и патчи:* Провайдеры облачных услуг обновляют программное обеспечение и операционные системы своих серверов регулярно для устранения уязвимостей и обеспечения безопасности.
- *Резервное копирование и восстановление:* Регулярные резервные копии данных на случай утери информации или атак позволяют восстановить данные в случае чрезвычайных ситуаций.
- *Управление доступом и политики безопасности:* Реализация строгих правил доступа и политик безопасности помогает предотвратить несанкционированный доступ к данным и системам.

Защита облачных серверов требует постоянного внимания и обновлений, учитывая постоянно меняющуюся среду угроз и появление новых видов киберугроз. Это делает безопасность данных в облаке важным аспектом для организаций и пользователей, использующих облачные сервисы.

Преимущества и недостатки методов защиты:

1. CD-ключи:

Преимущества: CD-ключи были широко используемы для проверки подлинности игры при установке или запуске.

Недостатки: Они стали менее эффективными из-за возможности создания поддельных или уникальных ключей.

2. Простые античиты:

Преимущества: Легко внедрить в игру, проверяют целостность игрового процесса на наличие изменений.

Недостатки: Часто обходимы пиратами, не дают полной защиты.

3. Динамическая античит-система:

Преимущества: Активно сканирует процессы в игре на наличие читов и мошеннической активности в реальном времени.

Недостатки: Может требовать больших вычислительных ресурсов и повышенной загрузки серверов.

4. Denuvo:

Преимущества:

А) Высокий уровень защиты: Denuvo обладает высокой степенью защиты от взлома и обхода защиты, что делает его одним из наиболее эффективных методов защиты.

Б) Обновления защиты: Регулярные обновления позволяют адаптировать защиту к новым методам взлома.

Недостатки:

А) Возможное влияние на производительность: Некоторые игроки сообщают о возможном снижении производительности из-за работы Denuvo.

Б) Уязвимость к взлому: Несмотря на высокую защиту, Denuvo все же был взломан в отдельных случаях, что создает риск для защищаемого контента.

5. Steam DRM:

Преимущества:

А) Интеграция с популярной игровой платформой: Steam DRM предоставляет интегрированную защиту для игр на платформе Steam.

Б) Удобство для пользователей: Покупка и активация игр осуществляются через одну платформу, что удобно для пользователей.

Недостатки:

А) Ограничения доступа: Некоторые игроки высказывают неудовлетворенность ограничениями доступа к играм и возможности запуска игр без подключения к интернету.

Б) Не всегда эффективен: Steam DRM также подвержен обходу и взлому, особенно для игр, которые не требуют подключения к Steam для запуска.

6. Защита облачных серверов:

Преимущества:

А) Защита ключевых компонентов игры: Помимо защиты самой игры, защита серверов также играет важную роль в предотвращении несанкционированного доступа.

Недостатки:

А) Необходимость постоянного соединения: Зависимость от облачных серверов может быть проблемой, особенно для одиночных игр или игр с ограниченным онлайн-режимом.

Б) Уязвимость к атакам: Облачные серверы также могут быть целью хакерских атак, что создает угрозу для безопасности игровой среды.

Каждый из этих методов имеет свои преимущества и недостатки, и часто компании используют комбинацию нескольких методов для повышения уровня защиты своего игрового контента.

Перспективы и будущее защиты от пиратства в играх:

Перспективы и будущее защиты от пиратства в играх привязаны к постоянному развитию технологий, стремлению создателей игр обеспечить надёжность и удобство для легальных пользователей, а также борьбе с пиратством[3]. Несмотря на постоянные усилия разработчиков, пираты находят новые способы обхода защиты, что заставляет индустрию игр постоянно развиваться и совершенствовать свои методы защиты.

Вот некоторые направления, которые могут определить будущее защиты от пиратства в играх:

1. Использование Искусственного Интеллекта (ИИ) и Машинного Обучения (МО): ИИ и МО могут играть важную роль в защите от пиратства, предоставляя способы обнаружения необычного поведения или паттернов, связанных с пиратскими действиями. Алгоритмы могут анализировать данные об игровом процессе и обнаруживать аномалии, что поможет предотвратить мошеннические попытки.

2. Усиленное шифрование и защита данных: Сложные алгоритмы шифрования и защиты данных могут обеспечить более надежную защиту от попыток взлома или изменения игровых файлов. Это также может предотвратить несанкционированный доступ к контенту игры.

3. Облачные технологии и потоковая передача: Переход к облачным игровым сервисам и потоковой передаче игр может уменьшить уязвимости, связанные с локальными файлами и дисками. Потоковая передача позволяет хранить часть игрового контента в защищённых облаках, что усложняет доступ для нелегального использования.
4. Комбинация методов защиты: Комбинирование нескольких методов защиты может стать более эффективным в борьбе с пиратством. Это может включать в себя обфускацию кода, динамическую античит-систему, криптографию данных и анализ поведения игроков.
5. Постоянное развитие и обновления: Разработчики игр должны постоянно обновлять и совершенствовать методы защиты, учитывая появление новых угроз и пиратских методов. Регулярные патчи и обновления позволяют быстро исправлять уязвимости и улучшать защиту.

Будущее защиты от пиратства в играх напрямую зависит от способности индустрии адаптироваться и развиваться, учитывая появление новых технологий и улучшение методов пиратства.

Выводы

Защита от пиратства в играх остаётся актуальной проблемой в индустрии разработки игр. Пираты постоянно ищут новые способы обхода защиты, требуя от разработчиков игр постоянного совершенствования методов защиты и применения новых технологий.

В ходе данного исследования были рассмотрены классические и современные методы защиты от пиратства. Классические методы, такие как CD-ключи и простые античиты, несмотря на свою простоту, стали менее эффективными из-за возможности быстрого обхода. Современные методы, такие как динамическая античит-система, шифрование данных и методы машинного обучения, обещают более надежную защиту, но зачастую требуют больших финансовых и временных затрат на их разработку и внедрение.

Однако, не существует универсального решения, которое обеспечило бы абсолютную защиту от пиратства. Вместо этого, эффективность защиты от пиратства в играх зависит от сочетания различных методов защиты, регулярных обновлений и постоянного мониторинга уязвимостей.

Будущее защиты от пиратства будет тесно связано с применением новых технологий, таких как искусственный интеллект, машинное обучение и облачные технологии, а также с постоянным совершенствованием существующих методов. Разработчики игр должны продолжать стремиться к созданию сбалансированной системы защиты, которая обеспечивает надёжность и безопасность игрового контента, сохраняя при этом комфорт и удовлетворение для законных пользователей.

Список литературы

1. Slabykh I. The New Approaches to Digital Anti-Piracy in the Entertainment Industry //UIC Rev. Intell. Prop. L. – 2019. – Т. 19. – 75с.
2. Zhang X. et al. Argus: A Fully Transparent Incentive System for Anti-Piracy Campaigns //2021 40th International Symposium on Reliable Distributed Systems (SRDS). – IEEE, 2021. – С. 143-153.
3. Karthik J., Amritha P. P., Sethumadhavan M. Video Game DRM: Analysis and Paradigm Solution //2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). – IEEE, 2020. – С. 1-4.

4. Hemnes T. Adaptation of Copyright Law to Video Games //U. Pa. L. Rev. – 1982. – Т. 131. – 171с.
5. Grosheide F. W., Roerdink H., Thomas K. Intellectual property protection for Video Games: A view from the European Union //J. Int't Com. L. & Tech. – 2014. – Т. 9. – 1с.

References

1. Slabykh I. The New Approaches to Digital Anti-Piracy in the Entertainment Industry //UIC Rev. Intell. Prop. L. – 2019. – Vol. 19. – p. 75.
2. Zhang X. et al. Argus: A Fully Transparent Incentive System for Anti-Piracy Campaigns //2021 40th International Symposium on Reliable Distributed Systems (SRDS). – IEEE, 2021. – pp. 143-153.
3. Karthik J., Amritha P. P., Sethumadhavan M. Video Game DRM: Analysis and Paradigm Solution //2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). – IEEE, 2020. – pp. 1-4.
4. Hemnes T. Adaptation of Copyright Law to Video Games //U. Pa. L. Rev. – 1982. – Vol. 131. – p. 171.
5. Grosheide F. W., Roerdink H., Thomas K. Intellectual property protection for Video Games: A view from the European Union //J. Int't Com. L. & Tech. – 2014. – Vol. 9. – p. 1.