DOI 10.46320/2077-7639-2025-3-136-61-66

Криптографические подходы к противодействию несанкционированному доступу к информационным системам онлайн-кинотеатров и их влияние на бизнес-показатели

Овчаренко А.А., Гершман М.А.

В условиях развития онлайн-кинотеатров их информационные системы сталкиваются с угрозой несанкционированного доступа – прежде всего пиратского копирования и распространения контента, а также кибератак, нацеленных на пользовательские данные. Одним из ключевых инструментов защиты в таких системах являются методы криптографии. В статье проведен обзор классических (AES, RSA, ГОСТ и др.) и современных криптографических подходов (постквантовые алгоритмы, гомоморфное шифрование и др.), применяемых для противодействия несанкционированному доступу к контенту и данным онлайн-кинотеатров. Проанализировано их влияние на бизнес-показатели: за счет снижения пиратства и повышения доверия пользователей обеспечение криптографической безопасности способствует росту выручки и аудитории легальных видеосервисов. Основное внимание уделено опыту российского рынка, действующим техническим решениям (DRM-системам, шифрованию трафика, авторизации) и законодательным мерам. Сделаны выводы о том, что применение криптографии является необходимым условием устойчивого развития индустрии онлайн-видео, а внедрение перспективных методов (квантовоустойчивых алгоритмов, полностью гомоморфного шифрования и пр.) в будущем позволит сохранить эффективность защиты в меняющихся условиях.

ДЛЯ ЦИТИРОВАНИЯ ГОСТ 7.1–2003

Овчаренко А.А., Гершман М.А. Криптографические подходы к противодействию несанкционированному доступу к информационным системам онлайн-кинотеатров и их влияние на бизнес-показатели // Дискуссия. — 2025. — Вып. 136. — С. 61–66.

КЛЮЧЕВЫЕ СЛОВА

Онлайн-кинотеатр, информационная безопасность, криптография, DRM, постквантовая криптография, гомоморфное шифрование, бизнес-модели, пиратство, защита контента, Россия.

DOI 10.46320/2077-7639-2025-3-136-61-66

Cryptographic approaches to counteracting unauthorized access to information systems of online cinemas and their impact on business indicators

Ovcharenko A.A., Gershman M.A.

In the context of online cinema development, their information systems face the threat of unauthorized access, primarily pirated copying and distribution of content, as well as cyberattacks aimed at user data. One of the key security tools in such systems is cryptography. The article provides an overview of classical (AES, RSA, GOST, etc.) and modern cryptographic approaches (post-quantum algorithms, homomorphic encryption, etc.) used to counteract unauthorized access to content and data of online cinemas. Their impact on business indicators is analyzed: by reducing piracy and increasing user confidence, cryptographic security contributes to the growth of revenue and audience of legal video services. The main attention is paid to the experience of the Russian market, current technical solutions (DRM systems, traffic encryption, authorization) and legislative measures. Conclusions are made that the use of cryptography is a necessary condition for the sustainable development of the online video industry, and the introduction of promising methods (quantum-resistant algorithms, fully homomorphic encryption, etc.) in the future will help maintain the effectiveness of protection in changing conditions.

FOR CITATION APA

Ovcharenko A.A., Gershman M.A. Cryptographic approaches to counteracting unauthorized access to information systems of online cinemas and their impact on business indicators. *Diskussiya [Discussion]*, 136, 61–66.

KEYWORDS

Online cinema, information security, cryptography, DRM, post-quantum cryptography, homomorphic encryption, business models, piracy, content protection, Russia.

ВВЕДЕНИЕ

Онлайн-кинотеатры стали популярным способом легального просмотра видео. В России их ежемесячная аудитория – десятки миллионов, и треть населения платит за подписку. Однако индустрия сталкивается с проблемой: пиратство и кибератаки. По оценке Минкультуры, потери от интернет-пиратства в РФ достигают 40–70 млрд рублей ежегодно – это сопоставимо с объёмом всего легального рынка. Кроме того, платформы хранят данные миллионов пользователей, становясь целью киберпреступников.

Для защиты информации применяются криптографические методы: шифрование данных, ключи и аутентификация. Они лежат в основе DRM-технологий, препятствующих несанкционированному доступу. Но защита не должна мешать удобству сервиса – нужен баланс.

Цель исследования – проанализировать криптографические методы защиты информационных систем онлайн-кинотеатров и их влияние на бизнес-показатели.

Задачи исследования:

1) Изучить классические криптоалгоритмы (AES, RSA, ГОСТ и др.);

2) Рассмотреть современные методы (постквантовые, гомоморфное шифрование);

3) Обобщить используемые решения на рынке (DRM, управление ключами, трафик);

4) Оценить влияние технологий на снижение пиратства, рост аудитории, доверие пользователей и соблюдение законодательства.

МАТЕРИАЛЫ И МЕТОДЫ

Работа представляет собой обзор научной и отраслевой литературы по информационной безопасности медиасервисов. Использованы источники из РИНЦ и отраслевые отчёты.

Применены методы анализа и синтеза. Рассмотрены базовые криптографические алгоритмы (симметричные, асимметричные, хеш-функции) и их роль в обеспечении конфиденциальности и аутентичности. Также проанализированы DRM и системы условного доступа. На основе собранных данных дана оценка влияния криптографии на уровень пиратства и экономику онлайн-кинотеатров. Результаты оформлены в таблицах и графиках.

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА КОНТЕНТА В ОНЛАЙН-КИНОТЕАТРАХ

Ключевой ресурс онлайн-кинотеатров – медиаконтент, права на который приобретены у правообладателей. Его доставка осуществляется по сети, а без шифрования возможна утечка и незаконное распространение. Поэтому используется симметричное (AES-128) и асимметричное (RSA, ECC) шифрование: первый – для быстрого кодирования потока, второй – для безопасной передачи ключей. AES демонстрирует высокую скорость и стойкость по сравнению с RSA.

В таблице 1 представлены криптографические алгоритмы, используемые в системах видеосервисов.

Контроль доступа обеспечивается DRM и CAS – серверами, выдающими лицензии только авторизованным пользователям. При воспроизведении фильма система проверяет подписку и отправляет зашифрованный ключ. Без него контент недоступен.

CAS/DRM использует многоуровневую модель:

1. ***Контентный ключ*** (постоянный);
2. ***Сеансовый ключ*** (меняется, напр., раз в час);
3. ***Пакетный ключ*** (обновляется каждые 5 минут).

Даже при компрометации одного ключа защита остаётся эффективной. Кроме того, используются водяные знаки (watermarking), позволяющие отследить источник пиратской копии.

Для защиты персональных данных применяются хеширование паролей, шифрование платёжных реквизитов и HTTPS. Исследование Роскачества (2021) подтвердило, что российские онлайн-кинотеатры не допускают утечек незашифрованных данных – весь трафик защищён.

Таблица 1

Криптографические алгоритмы и их назначение

Алгоритм	Тип	Назначение	Примечание
AES-128	Симметричный	Шифрование видео	Высокая скорость, 128-бит ключ
RSA-2048	Асимметричный	Передача ключей, подпись	Надёжный, но медленный
ГОСТ 28147-89	Симметричный	Альтернатива AES в РФ	256-бит ключ
ECC (ECDH, ECDSA)	Асимметричный	Обмен ключами, аутентификация	Меньший размер ключей
HTTPS (TLS)	Гибридный	Шифрование соединения	Использует AES и RSA/ECC
Watermarking	Стеганография	Метки в видео	Помогает отслеживать утечки
CRYSTALS-Kyber	Постквантовый	Перспективная альтернатива RSA	Пока не внедрён
FHE	Гомоморфный	Обработка шифроданных	Очень медленный

Таблица 2

Многоуровневая система ключей CAS/DRM

Уровень	Назначение	Длительность	Применение
Контентный	Присваивается файлу	Постоянный	Базовый
Сеансовый	Генерируется на сессию	~1 час	Идентификация сессии
Пакетный	Шифрует сегменты	~5 мин	Защита от перехвата

СОВРЕМЕННЫЕ КРИПТОГРАФИЧЕСКИЕ ВЫЗОВЫ И МЕТОДЫ

Алгоритмы AES и RSA активно применяются, но с развитием квантовых компьютеров могут стать уязвимыми. Алгоритм Шора способен эффективно взламывать RSA и ECC, что стимулировало развитие постквантовой криптографии (PQC). В 2022–2023 гг. NIST утвердил алгоритмы CRYSTALS-Kyber (шифрование) и Dilithium (ЭЦП) как стандарт. Пока они не внедрены в онлайн-кинотеатрах, но в перспективе должны заменить существующие схемы. Например, Kyber способен защитить лицензионные ключи от квантового взлома.

Симметричные алгоритмы (AES, ГОСТ) и хеш-функции более устойчивы: для их атаки применяется лишь алгоритм Гровера, что компенсируется увеличением длины ключа (например, AES-256).

Перспективным направлением остаётся полностью гомоморфное шифрование (FHE), позволяющее обрабатывать данные в зашифрованном виде (например, для рекомендаций), но оно крайне медленно – до 100 000 раз медленнее AES (см. таблицу 3).

Таблица 3

Пропускная способность шифрования (МБ/с)

Метод	Скорость	Комментарий
AES-128	1000	Базовый уровень
RSA-2048	100	~10 раз медленнее
Kyber	50	~20 раз медленнее
FHE	0.01	~100 000 раз медленнее

Из-за ресурсоёмкости FHE пока применим лишь в задачах, где безопасность важнее скорости. Тем не менее, исследования продолжаются.

Дополнительно развиваются 3 алгоритма:

1) Secure Multi-Party Computation – безопасные распределённые вычисления;

2) Блокчейн – для децентрализованного управления лицензиями;

3) ИИ-мониторинг – для выявления атак и аномалий.

Интеграция ИИ и криптографии позволяет динамически реагировать на угрозы, например, за счёт адаптивной смены ключей.

РЕЗУЛЬТАТЫ

Криптографическая защита – необходимое условие функционирования онлайн-кинотеатров. Без неё контент моментально распространялся бы на пиратских сайтах. DRM-системы усложнили работу «профессиональных» пиратов: для получения ключей требуется взлом защищённых серверов или устройств.

Рост легальных просмотров объясняется не только улучшением сервиса, но и усилением защиты: Роскомнадзор ежегодно блокирует тысячи нелегальных сайтов. В результате доходы пиратских платформ снижаются, а всё больше пользователей выбирают платные сервисы.

В экономике криптография позволяет монетизировать премьеры и эксклюзивы: правообладатели охотнее сотрудничают с платформами, обеспечивающими защиту. Это даёт конкурентное преимущество и рост подписной базы. Данные TMT Consulting отражают рост российского рынка:

Таблица 4

Динамика выручки рынка онлайн-кинотеатров (TMT Consulting)

Год	Выручка, млрд руб.	Прирост
2018	~20 (оценочно)	–
2019	~28	+40%
2020	39	+39%
2021	55	+41%
2022	~70 (оценочно)	+28%

Рост в 2021 году (+41%) объясняется как пандемией, так и развитием подписной модели, зависящей от защиты контента. Надёжная криптография способствует росту ARPU и снижению оттока: зритель уверен в безопасности и легальности сервиса.

Есть и издержки: лицензии на DRM (например, Widevine, PlayReady), ресурсы на шифрование, регулярное обновление ключей и сертификатов – всё это требует затрат. Также DRM может ограничивать функциональность (например, офлайн-доступ или скриншоты), что вызывает недовольство у части пользователей. Однако сервисы стремятся минимизировать неудобства.

В целом выгоды от защиты превышают затраты: без неё возможны потери – утечки, штрафы, снижение доверия. Защита контента и данных становится не только технической необходимостью, но и фактором конкурентоспособности.

ЗАКЛЮЧЕНИЕ

Исследование подтверждает, что криптография – основа защиты информационных систем онлайн-кинотеатров. Она обеспечивает конфиденциальность контента, контроль доступа

и защиту пользовательских данных. Основу инфраструктуры составляют симметричные (AES, ГОСТ) и асимметричные (RSA, ECC) алгоритмы, объединённые в гибридные протоколы (например, TLS).

DRM- и CAS-системы применяют многоуровневые ключи и watermarking, что делает копирование затруднительным и поддерживает подписную модель: зрители платят за безопасный, защищённый контент.

Рост российского рынка подтверждает эффективность защиты. С появлением новых угроз (в том числе квантовых) необходимо внедрение постквантовых алгоритмов, усиление аутентификации (включая биометрию) и применение ИИ для обнаружения атак.

Онлайн-кинотеатры уже стали площадкой для внедрения передовой криптографии – эти вложения окупаются ростом доверия, защитой данных и стабильным развитием отрасли.

Список литературы

1. *Зараменских, Е. П., Шибанов, А. М.* Средства защиты медиаконтента в Интернете // Перспективы развития информационных технологий. – 2012. – № 7. – С. 187–189. – [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/sredstva-zaschity-mediakontenta-v-internete (дата обращения: 16.04.2025).
2. *Джураева, Д. Ш., Ганиев, А. А.* Построение системы защиты сетей IPTV от несанкционированного доступа // Молодой ученый. – 2016. – № 11(115). – С. 331–335. – [Электронный ресурс]. – Режим доступа: https://moluch.ru/archive/115/31100/ (дата обращения: 16.04.2025).
3. **Пиратам закрыли плеер** // Коммерсантъ. – 09.09.2019. – [Электронный ресурс]. – Режим доступа:https://www.kommersant.ru/doc/4134092 (дата обращения: 16.04.2025).
4. *Ширяев, Е. М., Голимблевская, Е. И., Ващенко, И. С., Кучуков, В. А.* Обзор полностью гомоморфного шифрования // Научные исследования молодых учёных: сб. статей VIII Междунар. науч.-практ. конф. – Пенза: МЦНС «Наука и Просвещение», 2020. – С. 63–69. – [Электронный ресурс]. – Режим доступа: https://naukaip.ru/wp-content/uploads/2020/12/MK-964-1.pdf (дата обращения: 16.04.2025).
5. *Акопян, А. Р., Аракелян, А. М., Воронцова, Ю. В., Крысов, В. В.* Проблемы цифровой трансформации кинопроката // E-Management. – 2021. – № 1. – С. 4–12. – [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/problemy-tsifrovoy-transformatsii-kinoprokata (дата обращения: 16.04.2025).
6. *Демидов, М. И.* ТСЗАП в сфере защиты цифрового контента: практический опыт создания веб-инструментов // Труды по интеллектуальной собственности. – 2021. – Т. 39, № 4. – С. 74–79. – DOI: 10.17323/tis.2021.13515.
7. *Иванова, К. В., Сальников, А. Ф., Мормуль Р. В.* Искусственный интеллект для контроля передачи данных в тактическом звене управления с использованием многослойного и многопотокового шифрования геопространственной обстановки // Вестник Пермского университета. Математика. Механика. Информатика. – 2023. – Вып. 2(61). – С. 65–71. DOI: 10.17072/1993-0550-2023-2-65-71.
8. *Лемешева, М.* Импортозамещение в стриминге: как российским онлайн-кинотеатрам выжить в условиях санкций? – Российская газета, 12.04.2022. – [Электронный ресурс]. – Режим доступа: https://rg.ru/2022/04/12/importozameshchenie-v-striminge-kak-rossijskim-onlajn-kinoteatram-vyzhit-v-usloviiah-sankcij.html (дата обращения: 16.04.2025).
9. *Антипов, А.* Постквантовая криптография – угроза и защита в эпоху квантовых вычислений – SecurityLab, 15.08.2024. – [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/analytics/551151.php (дата обращения: 16.04.2025).
10. *Яндекс.Практикум.* Шифрование информации: какие методы существуют и как помогают защитить данные – Блог Практикума, 12.03.2024. – [Электронный ресурс]. – Режим доступа: https://practicum.yandex.ru/blog/chto-takoe-shifrovanie-informacii/ (дата обращения: 16.04.2025).
11. *Неупокоева, Е.* Онлайн-кинотеатры признали безопасными – ComNews, 18.02.2021. – [Электронный ресурс]. – Режим доступа: https://www.comnews.ru/content/213183/2021-02-18/onlayn-kinoteatry-priznali-bezopasnymi (дата обращения: 16.04.2025).

References

1. *Zaramenskikh, E. P., Shibanov, A. M.* Means of protecting media content on the Internet // Prospects for the development of information technology. – 2012. – № 7. – Pp. 187-189. – [Electronic resource]. – Access mode: https://cyberleninka.ru/article/n/sredstva-zaschity-mediakontenta-v-internete (access date: 16.04.2025).
2. *Dzhuraeva, D. Sh., Ganiev, A. A.* Building a system to protect IPTV networks from unauthorized access // Young scientist. – 2016. – № 11 (115). – P. 331-335. – [Electronic resource]. – Access mode: https://moluch.ru/archive/115/31100/ (access date: 16.04.2025).
3. *The* player was closed for pirates // Kommersant. – 09.09.2019. – [Electronic resource]. – Access mode: https://www.kommersant.ru/doc/4134092 (access date: 16.04.2025).
4. *Shiryaev, E. M., Golimblevskaya, E. I., Vaschenko, I. S., Kuchukov, V. A.* Review of fully homomorphic encryption // Scientific research of young scientists: collection of articles of the VIII Int. scientific and practical. conf. – Penza: MCNS "Science and Education", 2020. – Pp. 63-69. – [Electronic resource]. – Access mode: https://naukaip.ru/wp-content/uploads/2020/12/MK-964-1.pdf (access date: 16.04.2025).
5. *Akopyan, A. R., Arakelian, A. M., Vorontsova, Yu. V., Krysov, V. V.* Problems of digital transformation of film distribution // E-Management. – 2021. – № 1. – Pp. 4-12. – [Electronic resource]. – Access mode: https://cyberleninka.ru/article/n/problemy-tsifrovoy-transformatsii-kinoprokata (access date: 04/16/2025).
6. *Demidov, M. I.* TSZAP in the field of digital content protection: practical experience in creating web tools // Works on intellectual property. – 2021. – Vol. 39. – № 4. – Pp. 74-79. – DOI: 10.17323/tis.2021.13515.
7. *Ivanova, K. V., Salnikov, A. F., Mormul, R. V.* Artificial intelligence for monitoring data transmission at the tactical control level using multilayer and multistream encryption of the geospa-

tial environment // Bulletin of Perm University. Mathematics. Mechanics. Computer Science. – 2023. – Issue. 2(61). – Pp. 65–71. – DOI: 10.17072/1993-0550-2023-2-65-71.

8. *Lemesheva, M.* Import substitution in streaming: how can Russian online cinemas survive under sanctions? // Rossiyskaya Gazeta, 12.04.2022. – [Electronic resource]. – Access mode: https://rg.ru/2022/04/12/importozameshchenie-v-striminge-kak-rossijskim-onlajn-kinoteatram-vyzhit-v-usloviiah-sankcij.html (access date: 16.04.2025).
9. *Antipov, A.* Post-quantum cryptography – threat and protection in the era of quantum computing – SecurityLab, 15.08.2024. – [Electronic resource]. – Access mode: https://www.securitylab.ru/analytics/551151.php (access date: 16.04.2025).
10. *Yandex.Practicum.* Information encryption: what methods exist and how they help protect data – Blog of Practicum, 12.03.2024. – [Electronic resource]. – Access mode: https://practicum.yandex.ru/blog/chto-takoe-shifrovanie-informacii/ (access date: 16.04.2025).
11. *Neupokoeva, E.* Online cinemas recognized as safe – ComNews, 18.02.2021. – [Electronic resource]. – Access mode: https://www.comnews.ru/content/213183/2021-02-18/onlayn-kinoteatry-priznali-bezopasnymi (access date: 16.04.2025).

Информация об авторах

Овчаренко А.А., аспирант Московского финансово-промышленного университета «Синергия». SPIN-код: 4933-3288. ORCID: 0009-0009-6287-0494 (г. Москва, Российская Федерация).

Гершман М.А., аспирант Московского финансово-промышленного университета «Синергия». ORCID: 0009-0003-4788-0770 (г. Москва, Российская Федерация).

Information about the authors

Ovcharenko A.A., postgraduate student at the Moscow University of Finance and Industry "Synergy". PIN code: 4933-3288. ORCHID: 0009-0009-6287-0494 (Moscow, Russian Federation).

Gershman M.A., postgraduate student at the Moscow University of Finance and Industry "Synergy". ORCHID: 0009-0003-4788-0770 (Moscow, Russian Federation).