

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2026.167.55 EDN: LJNUXS

ПОДХОД К ЛИЦЕНЗИРОВАНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ СЕРТИФИКАТОВ X.509: РАЗРАБОТКА И ПЕРСПЕКТИВЫ

Научная статья

Гульмамедов Н.В.[1, *]

[1] Петербургский государственный университет путей сообщения, Санкт-Петербург, Российская Федерация

* Корреспондирующий автор (whatever[at]center-dom.info)

Предложена: 20.08.2025; Принята: 30.04.2026; Опубликована: 18.05.2026

Аннотация

В настоящей статье представлено исследование современных подходов к лицензированию программного обеспечения (ПО), основанное на применении цифровых сертификатов формата X.509. Анализируются различные методы защиты интеллектуальной собственности — от традиционных решений вроде локальных алгоритмов и аппаратных ключей до инновационных технологий облачных сервисов. Детально рассматриваются плюсы и минусы каждого способа, особое внимание уделено разработке собственной инфраструктуры открытых ключей (PKI). Приводится подробная информация о создании тестового стенда, подтверждающего работоспособность предложенного решения. Исследуются возможные сценарии атак и предлагаются меры противодействия угрозам информационной безопасности. Итоги исследования позволяют сделать выводы о перспективах внедрения цифровых сертификатов в процесс лицензирования ПО, сформулированы конкретные рекомендации по повышению эффективности автоматизации процессов лицензирования и защите от несанкционированного копирования.

Ключевые слова: лицензирование программного обеспечения, цифровые сертификаты, информационная безопасность, авторские права на ПО, X509 сертификат.

AN APPROACH TO SOFTWARE LICENSING USING X.509 CERTIFICATES: DEVELOPMENT AND PROSPECTS

Research article

Gulmamedov N.V.[1, *]

[1] Petersburg State Transport University, Saint-Petersburg, Russian Federation

* Corresponding author (whatever[at]center-dom.info)

Suggested: 20.08.2025; Accepted: 30.04.2026; Published: 18.05.2026

Abstract

This article presents a study of modern approaches to software licensing based on the use of X.509 digital certificates. Various methods of intellectual property protection are analysed—ranging from traditional solutions such as local algorithms and hardware keys to innovative cloud service technologies. The pros and cons of each method are examined in detail, paying particular attention to the development of a proprietary public key infrastructure (PKI). Detailed information is provided on the creation of a test bed confirming the viability of the proposed solution. Possible attack scenarios are studied and measures to counter information security threats are suggested. The research results allow conclusions to be drawn regarding the prospects for implementing digital certificates in the software licensing process, and specific recommendations are formulated to improve the efficiency of licensing process automation and protection against unauthorised copying.

Keywords: software licensing, digital certificates, information security, software copyright, X.509 certificate.

Введение

Лицензии играют ключевую роль в защите интеллектуальной собственности, определяя порядок использования, модификации и распространения программных продуктов. Они защищают интересы создателей и предоставляют четкие инструкции по использованию программ для пользователей.

Однако в условиях глобального роста цифровизации, при распространении программных продуктов у авторов программного обеспечения, возникает необходимость выбора оптимального способа лицензирования, обеспечивающего адекватную защиту, удобство использования и минимальные экономические издержки. Важно учитывать такие факторы, как безопасность, простота эксплуатации и поддержка будущих расширений функционала. Основные методы лицензирования ПО: локальные алгоритмы, аппаратные ключи и онлайн-сервисы, имеют ряд недостатков и преимуществ. Применение цифровых сертификатов стандарта X.509, основанных на инфраструктуре открытых ключей, нетипично для целей лицензирования ПО, но представляет собой новое актуальное направление, сочетающее в себе высокий уровень криптографической защиты, возможность лицензирования без доступа к сети и совместимость с современными платформами. В связи с этим разработка и исследование подхода к лицензированию ПО на основе X.509-сертификатов является актуальной задачей в области информационной безопасности.

Анализ современных источников в области защиты прав на программное обеспечение от неправомерного использования показывает интерес исследователей к аппаратным способам защиты. В работе К. С. Цыцуры и А. И.

Потоловского электронный ключ определяется как мультиплатформенная инструментальная система, обеспечивающая не только контроль доступа, но и защиту алгоритмов от изучения и клонирования. Авторы отмечают, что современные аппаратные ключи эволюционировали от простых устройств аутентификации к полноценным хранилищам криптографических ключей. В исследовании А. С. Кравченко, С. В. Родина и Т. Е. Смоленцевой показываются возможные методы обхода аппаратной защиты, включая программную симуляцию ключей и модификацию кода программы. И другие проанализированные источники свидетельствуют о том, что современные подходы к защите ПО все чаще опираются на криптографические методы, традиционно ассоциируемые с инфраструктурой открытых ключей, что создает теоретическую и практическую базу для рассмотрения сертификатов X.509 как эффективного инструмента лицензирования, позволяющего объединить преимущества аппаратной защиты с гибкостью программно-определяемых политик доступа.

Целью данного исследования является повышение защищенности разрабатываемого ПО за счет внедрения в него системы лицензирования, основанной на сертификатах формата X509. Для достижения цели, были выполнены ряд задач:

1) рассмотрены актуальные способы защиты, их преимущества и недостатки;
2) разработан алгоритм лицензирования;
3) реализован прототип и проведены испытания.

Общее представление о лицензировании ПО

Лицензирование программного обеспечения — это процесс предоставления прав на использование программного продукта определённым способом. Лицензия определяет условия, на которых пользователи могут устанавливать, запускать, модифицировать и распространять ПО. Она защищает права разработчиков и владельцев интеллектуальной собственности, а также устанавливает правила поведения для пользователей.

При защите ПО важно найти баланс между защитой и уровнем значимости продукта. Чрезмерные меры защиты информации могут быть экономически нецелесообразными и усложнить использование ПО для легитимных пользователей, тогда как недостаточные меры оставляют ПО уязвимым к несанкционированному доступу.

В следующих разделах подробно рассмотрим каждый метод, выделив преимущества и недостатки.

Локальный алгоритм проверки лицензии

Локальный алгоритм проверки лицензии — это метод, при котором проверка легитимности ПО происходит непосредственно на устройстве пользователя без обращения к внешним серверам или базам данных. Рассмотрим преимущества и недостатки локального лицензирования в таблице 1.

Таблица 1 - Преимущества и недостатки локального лицензирования

DOI: https://doi.org/10.60797/IRJ.2026.167.55.1

№ п/п	Преимущества	Недостатки
1	Самодостаточность: Все необходимые данные для проверки находятся прямо на устройстве пользователя.	Повышен риск реверс-инжиниринга и перебора ключей.
2	Отсутствие необходимости подключения к интернету.	Трудоемкость управления ключами и файлами лицензий.

Аппаратные ключи лицензирования

Аппаратные средства для лицензирования ПО представляют собой физические устройства, которые контролируют доступ к программам и их функциональность. Внутри ключа содержится микросхема, которая хранит информацию о лицензии, такую как:

1. Уникальный идентификатор устройства.
2. Тип лицензии (пробная, полная, корпоративная и т.д.).
3. Срок действия лицензии.
4. Ограничения на использование (функциональные возможности и др.).

ПО взаимодействует с аппаратным ключом, запрашивая необходимую информацию для проверки лицензии. Если ключ присутствует, и информация соответствует установленным критериям, программа продолжает свою работу. В противном случае программа либо ограничивает функциональность, либо вообще прекращает работу. Рассмотрим преимущества и недостатки аппаратного лицензирования в таблице 2.

Таблица 2 - Преимущества и недостатки аппаратного лицензирования

DOI: https://doi.org/10.60797/IRJ.2026.167.55.2

№ п/п	Преимущества	Недостатки
1	Высокая степень защиты. Физическое устройство сложно	Физические ограничения. Ключ — это физическое устройство,

№ п/п	Преимущества	Недостатки
	скопировать или подделать, что снижает риск несанкционированного использования ПО.	которое можно потерять, сломать или забыть подключить.
2	Аппаратные ключи не требуют постоянного соединения с интернетом для проверки лицензии.	Изготовление и доставка аппаратных ключей увеличивает затраты на производство и распространение ПО.
3	Портативность. Такой ключ можно переносить с одного компьютера на другой, что полезно для мобильных сотрудников или в ситуациях, где требуется работа на разных машинах.	Неудобство для облачных решений и систем использующих виртуализацию.
4	Легкая интеграция. Многие производители предлагают SDK (Software Development Kit) для интеграции поддержки аппаратных ключей в ПО, что упрощает разработку и поддержку лицензируемых продуктов.	Риск устаревания интерфейсов. С развитием технологий интерфейсы подключения могут меняться (например, переход от USB-A к USB-C), что потребует замены старых ключей на новые. SDK могут устареть с течением времени, тормозить переход к новым технологиям.

Онлайн-лицензирование

Онлайн-сервисы для лицензирования ПО, также известные как серверы управления лицензиями, представляют собой платформы, предназначенные для автоматизации процессов выдачи, контроля и мониторинга использования лицензий на ПО. Рассмотрим преимущества и недостатки онлайн лицензирования в таблице 3.

Таблица 3 - Преимущества и недостатки онлайн лицензирования

DOI: https://doi.org/10.60797/IRJ.2026.167.55.3

№ п/п	Преимущества	Недостатки
1	Автоматизация процессов: Управление выдачей, продлением и контролем лицензий осуществляется автоматически, что экономит время и ресурсы разработчиков.	Зависимость от интернет-соединения: для работы большинства онлайн-сервисов необходимо стабильное подключение к интернету.
2	Масштабируемость: адаптируются под увеличение числа пользователей и новых продуктов, что удобно для растущих компаний.	Риск сбоев и уязвимостей: как любая онлайн-платформа, серверы лицензирования подвержены сбоям и уязвимостям, что может привести к временным простоям или утечке данных.
3	Удобство для пользователей: клиенты получают простой способ активации и продления лицензий, а также доступ к обновлениям и новым версиям ПО.	–

Подход с использованием сертификатов для лицензирования

В ходе исследования был проведен эксперимент с применением сертификатов X.509 для лицензирования программного обеспечения. Этот метод должен позволить значительно повысить уровень защиты продукта, эффективно управлять правами использования и обеспечить надежную идентификацию легальных пользователей продукта.

Проанализируем механизм функционирования данного подхода:

Сертификаты X.509 содержат информацию о владельце, публичных ключах и других атрибутах, связанных с пользователем или устройством. Эти данные хранятся внутри самого сертификата и защищены криптографическими методами. Рассмотрим Преимущества и недостатки использования сертификатов в таблице 4.

Таблица 4 - Преимущества и недостатки использования сертификатов

DOI: https://doi.org/10.60797/IRJ.2026.167.55.4

№ п/п	Преимущества	Недостатки
1	Цифровые сертификаты обеспечивают высокий уровень защиты от подделок и несанкционированного использования.	Сложность развертывания и администрирования: Настройка и поддержание инфраструктуры PKI требует ресурсов и знаний.
2	Сертификаты могут содержать различные параметры и условия лицензирования, что позволяет легко настраивать и управлять лицензиями для разных сценариев использования.	Требуется учесть возможные варианты обхода: изменение времени на локальном устройстве т.д.
3	Администраторы могут централизованно управлять лицензиями, обновляя и отзывая сертификаты по мере необходимости.	–
4	Совместимость. Сертификаты X.509 поддерживаются большинством современных платформ и сред выполнения.	–
5	Гибридный режим использования (оффлайн-онлайн). ПО не требуется постоянно проверять актуальность лицензии, так как срок актуальности записан в самом сертификате, требуется лишь проверка на отзыв сертификата.	–

Используемый алгоритм работы лицензирования на основе сертификатов

7.1. Выдача лицензии

Поставщик ПО генерирует сертификат X.509, содержащий информацию о лицензии, и передает его пользователю. Этот сертификат может быть передан различными способами, например, через электронную почту, загружен с сайта компании или получение встроено в сам продукт.

Для достижения поставленной цели требуется создать самоподписанный сертификат или взять имеющийся, сертификат, подписанный доверенным центром. Такой сертификат должен обладать возможностью подписывания сертификатов нижнего уровня иерархии. Общая иерархия сертификации показана на рисунке 1.

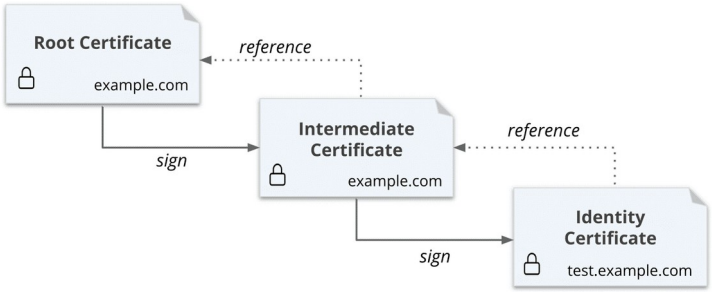

Рисунок 1 - Иерархия сертификации
DOI: https://doi.org/10.60797/IRJ.2026.167.55.5

После успешного создания центра сертификации переходим к выпуску сертификата «лицензии».

Для выпуска такой лицензии можно воспользоваться готовыми решениям в рамках PKI (Инфраструктура открытых ключей, англ. Public Key Infrastructure) или реализовать собственное решение. Для большей персонализации под конкретную задачу собственное решение может позволить добавлять расширения в сертификат. В данном исследование было использовано готовое решение.

Атрибуты сертификата:

1) основным идентифицирующим атрибутом является Serial Number;
2) поле CN содержит информацию о лицензии (номер);
3) в теле сертификата находится информация об организации;
4) срок действия лицензии;
5) открытый и закрытый ключи;
6) дополнительные атрибуты по требованию.

7.2. Установка и активация

Пользователь устанавливает ПО и предоставляет полученный сертификат. Программа проверяет сертификат на предмет его действительности и соответствия требованиям лицензии. Если проверка успешна, программа активируется и начинает функционировать согласно условиям лицензии.

7.3. Проверка лицензии

Программа периодически проводит проверку лицензии, используя сертификат X.509. Она может проверять следующие аспекты:

- срок действия лицензии. Если срок истек, программа уведомляет пользователя о необходимости продления или заблокировать определенные функции;
- право на использование. Проверяется соответствие лицензии текущему состоянию программы (например, число активных пользователей, объем используемых ресурсов, текущее устройство и т.п.);
- актуальность сертификата на сервере лицензирования. Проверять не был ли отозван сертификат на стороне сервера лицензирования. Например, за нарушение лицензионных требований.

7.4. Механизм отзыва сертификата

Механизм отзыва сертификата представляет собой процесс дистанционного вывода из эксплуатации переданной копии программного обеспечения. Для получения информации о статусе лицензии, клиентское ПО отправляет запрос на сервер лицензирования. Данный механизм позволяет производить отзыв сертификата с минимальными затратами и максимальной оперативностью. Обоснованность выбора в сторону данного механизма отзыва, а не проверку через список отозванных сертификатов является высокая скорость проверки при большом списке отозванных сертификатов и отсутствие временной задержки при обновлении такого списка. В случае недоступности сервера проверки сертификатов, будут работать только уже активированные копии, новая активация будет недоступна.

Тестирование прототипа

Для проверки и демонстрации работоспособности предлагаемого подхода к лицензированию, был создан прототип сервера лицензирования. Сервер был построен на платформе .Net ASP Net Core. Проведем следующие тесты:

- время создания сертификата и отправка его клиенту;
- время успешной проверки сертификата;
- время неудачной проверки сертификата, по разным причинам: некорректный номер лицензии, идентификатор устройства или отозванный сертификат.

В таблице 5 и на рисунке 2 показаны результаты тестирования.

Таблица 5 - Результаты тестирования

DOI: https://doi.org/10.60797/IRJ.2026.167.55.6

№ п\п	Создание сертификата, мс.	Проверка успешная, мс.	Проверка с ошибкой, мс.
1	442	72	149
2	313	67	101

№ п\п	Создание сертификата, мс.	Проверка успешная, мс.	Проверка с ошибкой, мс.
3	375	73	36
4	381	67	35
5	390	75	37

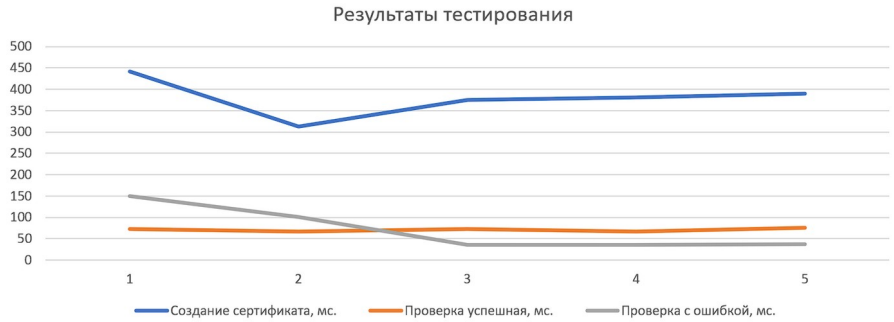

Рисунок 2 - Результаты тестирования
DOI: https://doi.org/10.60797/IRJ.2026.167.55.7

Анализ угроз и мер противодействия

Предлагаемый подход лицензирования значительно повышает надежность защиты ПО, однако остается подверженным потенциальным рискам и угрозам. В таблице 6 рассмотрим более подробно возможные сценарии атак и соответствующие меры предотвращения таких атак.

Таблица 6 - Возможные векторы атак и риски

DOI: https://doi.org/10.60797/IRJ.2026.167.55.8

Тип атаки	Условия и последствия	Меры по предотвращению
Компрометация закрытого ключа	Атака возможна, если злоумышленники получат доступ к закрытому ключу сертификационного центра.	Хранение закрытого ключа в защищенном формате, строгое ограничение доступа сотрудников к чувствительным данным.
Изменение локального времени на клиентском устройстве	Пользователь может изменить системное время компьютера, чтобы обойти проверку срока действия сертификата.	В клиентском приложении проводить онлайн-валидацию времени через NTP-серверы.
Атаки типа «Человек посередине»	Сетевые атаки при проверке статуса лицензии через интернет, целью которых является перехват трафика между клиентом и сервером лицензирования.	Шифрование канала связи с использованием протокола TLS версии 1.3.
Подделка сертификатов	Попытка создания собственных сертификатов с целью выдавать себя за владельца лицензии.	При создании сертификата, он подписывается с помощью вышестоящего (корневого и промежуточного) сертификата. Хэш алгоритм подписи SHA256. Проверка серийного номера корневого сертификата.

Заключение

Проведенное исследование посвящено разработке и реализации метода лицензирования программного обеспечения (ПО) с использованием цифровых сертификатов формата X.509. Данный подход направлен на повышение уровня безопасности и удобства управления правами доступа к программным продуктам.

Основные выводы и результаты исследования:

1. Эффективность и надежность. Использование сертификатов X.509 обеспечивает высокий уровень защиты благодаря криптографической аутентификации и контролю целостности данных. Это снижает риски фальсификации и незаконного распространения ПО.

2. Централизация управления. Администраторы имеют возможность централизованного управления лицензиями путем обновления и отзыва сертификатов, что упрощает администрирование больших инфраструктур.

3. Интеграция и совместимость. Формат X.509 поддерживается практически всеми современными операционными системами и приложениями, обеспечивая высокую гибкость и масштабируемость решений.

4. Практическая реализация. Проведен успешный эксперимент по созданию инфраструктуры публичного ключа (PKI) и интеграции сертификатов в процессы лицензирования. Эксперимент подтвердил работоспособность предложенного решения.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. X.509 certificates // Microsoft Learn. — 2023. — URL: https://learn.microsoft.com/en-us/azure/iot-hub/reference-x509-certificates. (дата обращения: 01.08.25)

2. Горбатов В.С. Основы технологии PKI / В.С. Горбатов, О.Ю. Полянская. — Москва : Горячая линия – Телеком, 2004. — 248 с.

3. RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. — Introd. 2008-05-01. — IETF, 2008. — 151 p.

4. Васильева И.Н. Криптографические методы защиты информации / И.Н. Васильева. — Москва : Юрайт, 2025. — 310 с.

5. Мельников В.В. Основы информационной безопасности : учебное пособие / В.В. Мельников. — Москва : Российский государственный университет правосудия, 2025. — 220 с.

6. Белов Е.Б. Основы информационной безопасности : учебное пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков и др. — Москва : Горячая линия-Телеком, 2011. — 558 с.

7. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности / Ю.И. Коваленко. — Москва : Горячая линия-Телеком, 2012. — 140 с.

8. Баранова Е.К. Основы информационной безопасности : учебник / Е.К. Баранова, А.В. Бабаш. — Москва : ИНФРА-М, 2025. — 202 с.

9. Кравченко А.С. Аппаратно-программные средства и информационные процессы защиты систем предоставления пользователям доступа к программным ресурсам / А.С. Кравченко, С.В. Родин, Т.Е. Смоленцева // Современные проблемы науки и образования. — 2015. — № 1. — URL: https://science-education.ru/ru/article/view?id=19158 (дата обращения: 01.12.25).

10. Цыцура К.С. Технология защиты от несанкционированного использования программного обеспечения «Электронный ключ» / К.С. Цыцура, А.И. Потоловский // Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева». — 2016. — № 12. — С. 664–666.

Список литературы на английском языке / References in English

1. X.509 certificates // Microsoft Learn. — 2023. — URL: https://learn.microsoft.com/en-us/azure/iot-hub/reference-x509-certificates. (accessed: 01.08.25)

2. Gorbatov V.S. Osnovi tekhnologii PKI [Fundamentals of PKI technology] / V.S. Gorbatov, O.Yu. Polyanskaya. — Moscow : Goryachaya liniya – Telekom, 2004. — 248 p. [in Russian]

3. RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. — Introd. 2008-05-01. — IETF, 2008. — 151 p.

4. Vasileva I.N. Kriptograficheskie metodi zashchiti informatsii [Cryptographic Methods of Information Protection] / I.N. Vasileva. — Moscow : Yurait, 2025. — 310 p. [in Russian]

5. Melnikov V.V. Osnovi informatsionnoi bezopasnosti [Fundamentals of Information security] : a study guide / V.V. Melnikov. — Moscow : Rossiiskii gosudarstvennii universitet pravosudiya, 2025. — 220 p. [in Russian]

6. Belov Ye.B. Osnovi informatsionnoi bezopasnosti : uchebnoe posobie [Fundamentals of Information Security : a study guide] / Ye.B. Belov, V.P. Los, R.V. Meshcheryakov et al. — Moscow : Goryachaya liniya-Telekom, 2011. — 558 p. [in Russian]

7. Kovalenko Yu.I. Pravovoi rezhim litsenzirovaniya i sertifikatsii v sfere informatsionnoi bezopasnosti [The legal regime of licensing and certification in the field of information security] / Yu.I. Kovalenko. — Moscow : Goryachaya liniya-Telekom, 2012. — 140 p. [in Russian]

8. Baranova Ye.K. Osnovi informatsionnoi bezopasnosti [Fundamentals of information security] : textbook / Ye.K. Baranova, A.V. Babash. — Moscow : INFRA-M, 2025. — 202 p. [in Russian]

9. Kravchenko A.S. Apparatno-programmnie sredstva i informatsionnie protsessi zashchiti sistem predostavleniya polzovatelyam dostupa k programmnim resursam [Hardware and software tools and information processes for protecting systems that provide access to software resources for users] / A.S. Kravchenko, S.V. Rodin, T.E. Smolentseva // Sovremennie problemi nauki i obrazovaniya [Modern problems of science and education]. — 2015. — № 1. — URL: https://science-education.ru/ru/article/view?id=19158 (accessed: 01.12.25). [in Russian]

10. Tsitsura K.S. Tekhnologiya zashchiti ot nesanktsionirovannogo ispolzovaniya programmnogo obespecheniya «Elektronnii klyuch» [Technology protection against unauthorized use of the software «Electronic key»] / K.S. Tsitsura, A.I. Potolovskii // Federalnoe gosudarstvennoe byudzhetnoe obrazovatelnoe uchrezhdenie visshego obrazovaniya «Sibirskii gosudarstvennii universitet nauki i tekhnologii imeni akademika M. F. Reshetneva» [Federal State Budgetary Educational Institution of Higher Education "Reshetnev Siberian State University of Science and Technology"]. — 2016. — № 12. — P. 664–666. [in Russian]