Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056

ГЕРАСИМОВ
Вячеслав Александрович

УСОВЕРШЕНСТВОВАННЫЙ ПРОТОКОЛ ВЫРАБОТКИ ОБЛАЧНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Автореферат
на соискание степени магистра
по специальности 1–40 80 02 Системный анализ, управление и обработка информацией (системы управления информацией)

_____

Научный руководитель
доцент, кандидат технических наук
БОЙПРАВ Ольга Владимировна

_____

Минск 2024

ВВЕДЕНИЕ

В последние годы наблюдается активное развитие облачных сервисов, которые позволяют пользователям получать доступ к файлам и приложениям с любого устройства, будь то мобильный телефон или компьютер.

В рамках облачных сервисов хранение данных и выполнение вычислений производится не на локальных устройствах, а на удаленных серверах. Примерами облачных сервисов являются Google Drive и Dropbox для хранения файлов, Gmail – для электронной почты, Microsoft Office 365 – для офисных приложений и AWS Cloud9 для разработки программного обеспечения.

Использование облачных сервисов в настоящее время характеризуется рядом преимуществ:

– повышение гибкости работы организаций, поскольку сотрудники могут легко получать доступ к необходимым данным и приложениям независимо от своего местоположения;

– сокращение расходов организаций на поддержание собственных серверов, т. к. обработка данных осуществляется на удаленных серверах, доступ которым обеспечивается по правилам, заложенным в основу модели «оплат за использование».

Термин «облако» возник в индустрии высоких технологий и используется для обозначения сетевой инфраструктуры и серверов Интернета. Его происхождение связано с тем, что на технических схемах часто изображались серверы и сетевая инфраструктура в виде облака. С появлением тенденции перемещения вычислительных процессов с локальных серверов на удаленные, специалисты стали использовать термин «облако» для краткого обозначения места, где происходят эти вычисления. В настоящее время под «облаком» понимается совокупность серверов, программного обеспечения и баз данных, доступ к которым осуществляется через Интернет и которые используются для выполнения программ и хранения данных от имени удаленного пользователя.

Разработка облачных сервисов стала возможной благодаря технологии виртуализации. Эта технология позволяет создавать на компьютере виртуальные среды, которые функционируют подобно отдельным физическим компьютерам с собственным оборудованием. Такие среды называются виртуальными машинами. При правильной настройке виртуальные машины, размещенные на одном физическом компьютере, изолированы друг от друга. Они не могут взаимодействовать друг с другом, и файлы и приложения одной виртуальной машины недоступны для других виртуальных машин.

Применение виртуальных машин позволяет организовать эффективное

использование серверного оборудования, так как при одновременном запуске множества виртуальных машин на одном сервере он может выступать как множество логически независимых серверов, использующих одно и то же оборудование. Это позволяет поставщикам облачных сервисов предлагать использование своих серверов гораздо бóльшему количеству клиентов одновременно, чем они могли бы предложить без использования виртуализации.

В настоящее время одним из популярных облачных сервисов является сервис облачной электронной цифровой подписи, который предполагает удаленную выработку электронной цифровой подписи. При использовании этого сервиса личный ключ, используемый для создания подписи, хранится и управляется удаленным сервером от имени подписанта. Для обеспечения безопасного процесса создания подписи и предоставлений гарантий контроля над личным ключом подписанта, поставщик услуг по удаленной выработке подписи должен применять специальные механизмы безопасности и использовать защищенное аппаратное и программное обеспечение, а также защищенный канал связи с подписантом.

В связи с вышеизложенным можно констатировать, что исследования, посвященные информационным системам, в которых используется облачная электронная подпись, являются актуальным.

Цель настоящей работы – анализ современных подходов к выработке облачной электронной цифровой подписи и разработка по результатам этого анализа усовершенствованного протокола выработки такой подписи.

В ходе достижения цели были решены следующие задачи:

1) выполнение анализа особенностей построения и функционирования современных систем выработки облачной электронной цифровой подписи;

2) выбор требований к реализации механизмов безопасности в рамках усовершенствованного протокола выработки облачной электронной цифровой подписи;

3) определение порядка использования разработанного усовершенствованного протокола выработки облачной электронной цифровой подписи.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Тема магистерской диссертации утверждена приказом учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» от 05.10.2022 № 2311-с.

Тема диссертации соответствует приоритетным направлениям научной, научно-технической и инновационной деятельности на 2021–2025 годы,

утвержденным Указом Президента Республики Беларусь от 07.05.2020 № 156 (пункт 1 «Цифровые информационно-коммуникационные и междисциплинарные технологии, основанные на них производства», пункт 6 «Обеспечение безопасности человека, общества и государства»).

Исследования по теме магистерской диссертации выполнялись в рамках опытно-конструкторской работы «Совершенствование инфраструктуры открытых ключей на основе современных web-технологий» по мероприятию 2 программы Союзного государства «Совершенствование системы защиты информационных ресурсов Союзного государства и государств участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» («Паритет»), утвержденной постановлением Совета Министров Союзного государства от 11 июня 2018 г № 5.

Работа выполнялась на базе учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» и на базе Научно-производственного республиканского унитарного предприятия «Научно-исследовательский институт технической защиты информации».

Цель и задачи исследования

Целью диссертационной работы является проведение анализа современных подходов к выработке облачной электронной цифровой подписи и разработка по результатам этого анализа усовершенствованного протокола выработки такой подписи.

Для достижения поставленной цели в диссертации решены следующие задачи:

1) выполнение анализа особенностей построения и функционирования современных систем выработки облачной электронной цифровой подписи;

2) предъявление требований к реализации механизмов безопасности в рамках усовершенствованного протокола выработки облачной электронной цифровой подписи;

3) определение порядка использования разработанного усовершенствованного протокола выработки облачной электронной цифровой подписи.

Личный вклад соискателя ученой степени

Личный вклад соискателя степени магистра в результаты диссертации заключается в проведении исследований, направленных на выбор требований к реализации механизмов безопасности в рамках усовершенствованного протокола выработки облачной электронной цифровой подписи, разработку и определение порядка использования разработанного протокола.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем кандидатом технических наук, доцентом О. В. Бойправ.

Магистр технических наук, ведущий инженер-программист Казловский М. А. определил проблематику аутентификации в системах электронного голосования, разработал протокол регистрации избирателя в системе электронного голосования с помощью системы облачной подписи и обосновал его надежность. Результаты, полученные соавтором, в диссертацию не вошли.

Апробация диссертации и информация об использовании ее результатов

Основные результаты диссертации докладывались и обсуждались на научных, научно-технический и научно-практических конференциях различного уровня: VIII конференция «Технологии защиты информации и информационная безопасность организаций» (IT-Security Conference) (г. Минск, 28–29 марта 2023 г.); XXVIII научно-практическая конференция «Комплексная защита информации» (г. Гомель, 23–25 мая 2023 г.); XXI Белорусско-российская научно-техническая конференция «Технические средства защиты информации» (г. Минск, 6 июня 2023 г.); IX конференция «Технологии защиты информации и информационная безопасность организаций» (IT-Security Conference) (г. Минск, 27–28 марта 2024 г.); XXIX научно-практическая конференция «Комплексная защита информации» (г. Санкт-Петербург, 15–17 мая 2024).

Результаты диссертационной работы используются при разработке научно-технической продукции в Научно-производственном республиканском унитарном предприятии «Научно-исследовательский институт технической защиты информации».

Опубликование результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 7 печатных работ общим объемом 3 авторских листа, в том числе 3 статьи в научных журналах, соответствующих пункту 19 Положения о присуждении ученых степеней и присвоении ученых званий, 3 статьи и 1 тезис в сборниках материалов конференций.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав с выводами по каждой главе, заключения, библиографического списка, пяти приложений.

Общий объем диссертационной работы составляет 84 страницы, из них 53 страницы текста, 7 рисунков на 6 страницах, 8 таблиц на 8 страницах, список использованных источников (31 наименование на 2 страницах), список публикаций автора по теме диссертации (7 наименований на 1 странице), 5 приложений на 10 страницах.

Проверка на уникальность

Проведена экспертиза диссертации Герасимова Вячеслава Александровича «Усовершенствованный протокол выработки облачной электронной цифровой подписи» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: https://antiplagiat.ru) в on-line режиме 12.05.2024 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 82,09 %).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрены проблемы необходимости проведения исследований, посвященных информационным системам, в которых используется облачная электронная подпись.

В **общей характеристике работы** показана связь работы с приоритетными направлениями научных исследований, цель и задачи исследования, личный вклад соискателя ученой степени, апробация результатов диссертации.

В первой главе рассмотрены и классифицированы модели облачных сервисов. Рассмотрен опыт внедрения удаленной электронной подписи в Европейском союзе с использованием приложения «Handy-Signatur». Представлены различные способы аутентификации в HSM с помощью OTP, QR-кода модуля SE. Рассмотрена возможность использования облачной электронной цифровой подписи в качестве услуги с помощью протокола, в котором учувствуют три стороны (подписант или эмитент, прокси-сервер и HSM) для безопасной генерации значения электронной цифровой подписи. Представлены механизмы защиты от подмены подписываемого документа в процессах отображения и подписи. Проанализирована международная система облачной подписи TW4S и определены функции каждого компонента, входящего в данную систему. Рассмотрены существующие решения, предоставляющие возможности по выработке электронной цифровой подписи с использованием облачных технологий и механизмов повышения доверия.

Во второй главе сформулированы подходы к усовершенствованию протокола выработки облачной электронной цифровой подписи. Описаны основные компоненты протокола выработки облачной электронной цифровой подписи. Рассмотрены подходы к идентификации и аутентификации.

Сформулированы требования, предъявляемые к системе облачной подписи при идентификации и аутентификации подписи подписанта согласно уровням гарантий контроля. Рассмотрены подходы к управлению ключами. Сформулированы требования, которые необходимо соблюдать при управлении криптографическими ключами, используемыми в системах облачной подписи. Рассмотрены подходы к формированию электронных документов, созданных с помощью систем облачной подписи. Сформулированы требования, которые необходимо соблюдать при формировании электронных документов, созданных с помощью систем облачной подписи. Представлены механизмы защиты информации, позволяющие обеспечить прозрачное и безопасное функционирование системы облачной подписи при выработке значения последней.

В третьей главе представлен разработанный усовершенствованный протокол активации подписи, в котором реализованы механизмы: идентификация и аутентификация подписанта, управление личным ключом подписанта, формирование электронных документов, созданных с помощью системы облачной электронной цифровой подписи, защита информации при выработке облачной электронной цифровой подписи.

Представлено описание разработанного протокола в виде алгоритма, в виде словесного описания по шагам, а также в виде схемы. Представлены криптографические механизмы, используемые в разработанном протоколе. Представлены результаты анализа применимости атак, основанных на обходе идентификации и аутентификации, механизмов управления ключами и формирования электронных документов.

Предложено применять разработанный протокол в системах электронного голосования, в интегрированной информационной системе «БГУИР: Университет» и в автоматизированной информационной системе «электронный рецепт».

В четверной главе рассмотрен шаблон канвы бизнес-модели, согласно методологии Александра Остервальдера, приведена канва бизнес-модели для проекта «Система облачной подписи», представлены результаты анализа существующих на рынке Республики Беларусь решений, предоставляющих возможность создавать электронный документ с помощью электронной подписи, использовать электронную подпись в процессе аутентификации.

ЗАКЛЮЧЕНИЕ

В процессе работы над магистерской диссертацией был проведен анализ современных систем выработки облачной электронной цифровой подписи. Были рассмотрены модели облачных сервисов, подходы к реализации облачной электронной цифровой подписи. Были рассмотрены уже существующие решения, их основные возможности. Была рассмотрена

основная структура системы облачной подписи, были выделены основные компоненты и требования
к каждому компоненту системы облачной подписи.

На основании полученных данных по итогам анализа, были сформулированы требования для усовершенствованного протокола выработки облачной электронной цифровой подписи в части идентификации и аутентификации, управлению ключами, формированию электронного документа, механизмов защиты информации при непосредственной выработке значения облачной электронной цифровой подписи.

По итогам разработки усовершенствованного протокола выработки облачной электронной цифровой подписи был проведен сравнительный анализ с уже существующими решениями, такими как Cloud Signature Consorcium, был проведен анализ применимости атак на разработанный протокол. Было предложено прикладное использование разработанного протокола в системах электронного голосования и интегрированной информационной системе.

Разработанный протокол активации облачной электронной цифровой подписи прошел экспертную оценку стойкости в учреждении Белорусского государственного университета «Научно-исследовательский институт прикладных проблем математики и информатики».

В последующем исследования по данной теме будут направлены на:

– совершенствование механизмов защиты информации в системе облачной подписи;

– усовершенствование разработанного протокола активации подписи для использования без прикладной системы, что позволит работать с электронным документом непосредственно в клиентской программе пользователя;

– усовершенствование принципа «Что вижу, то и подписываю» для всех форматов документов.

Внедрение разработанного программного комплекса с возможностью выработки облачной электронной цифровой подписи позволит повысить эффективность функционирования информационных систем инфраструктуры открытых ключей Республики Беларусь. Для организаций, переход на «облачные» сервисы позволит повысить гибкость бизнес-процессов, оптимизировать организацию работы сотрудников и сократить затраты на владение аппаратным обеспечением.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в рецензируемых научных журналах

1–А. Герасимов, В. А. Алгоритм разработки и методика использования в учебном процессе программного средства для преобразования информации / В. А. Герасимов, О. В. Бойправ // Цифровая трансформация. – 2023. – Т. 29, № 4. – С. 41–49. – https://doi.org/10.35596/1729-7648-2023-29-4-41-49.

2–А. Герасимов, В. А. Использование системы облачной электронной подписи для организации электронного голосования / В. А. Герасимов, М. А. Казловский // Цифровая трансформация. – 2024. – Т. 30, № 1. – С. 52–62. http://dx.doi.org/10.35596/1729-7648-2024-30-1-52-62.

3–А. Герасимов, В. А. Метод обнаружения событий информационной безопасности в системах облачной подписи / В. А. Герасимов, О. В. Бойправ // Цифровая трансформация. – 2024. – Т. 30, № 2. – С. 77–84. http://dx.doi.org/10.35596/1729-7648-2024-30-2-77-84.

Статьи в сборниках материалов конференций

4–А. Герасимов, В. А. Механизмы защиты информации при выработке облачной электронной цифровой подписи / В. А. Герасимов, М. А. Казловский, О .В. Бойправ // Комплексная защита информации: материалы XXVIII научно-практической конференции, г. Гомель, 23–25 мая 2023 г. / Белорусский государственный университет транспорта. – Гомель, 2023. – С. 257–261.

5–А. Герасимов, В. А. Подходы к использованию системы облачной электронной цифровой подписи в Республике Беларусь / В. А. Герасимов // Комплексная защита информации: материалы XXIX научно-практической конференции, г. Санкт-Петербург, 15 – 17 мая 2024 г. (в печати).

6–А. Герасимов, В. А. Итоги проекта «Система облачной подписи» в Республике Беларусь / В. А. Герасимов, Д. А. Арестович // Комплексная защита информации: материалы XXIX научно-практической конференции, г. Санкт-Петербург, 15 – 17 мая 2024 г. (в печати).

Тезисы докладов

7–А. Герасимов, В. А. Программный комплекс регистрационного центра инфраструктуры открытых ключей с механизмом выработки облачной электронной цифровой подписи / В. А. Герасимов // Технические средства защиты информации : тезисы докладов XXI Белорусско-российской научно-технической конференции, Минск, 6 июня 2023 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Т. В. Борботько [и др.]. – Минск, 2023. – С. 27–28.