УДК 004.056.53

В. Д. Сергеев
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Р. Р. Фаткиева
Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Метод двухфакторной аутентификации в облачном сервисе

Рассмотрены существующие методы аутентификации, проведен их сравнительный анализ. Исходя из специфики защищаемой системы, определен ряд требований к разрабатываемому механизму аутентификации. Предложен метод двухфакторной аутентификации по электронному ключу, представляющему собой электронный носитель, обладающий некоторыми аппаратными характеристиками, которые также выступают в роли дополнительного фактора аутентификации, с записанным на нем секретом, и одноразовому шестизначному цифровому паролю, передаваемому на мобильное устройство пользователя по SMS-каналу. Осуществлен выбор и дальнейшая настройка инфраструктуры для программной реализации системы аутентификации и проведена имплементация полученного алгоритма. Представлена архитектура системы аутентификации, реализованная в виде клиент-серверного приложения. В результате получено программное решение, повышающее защищенность доступа пользователей к облачному сервису. В рамках дальнейшей оптимизации предложены мероприятия по улучшению архитектуры системы двухфакторной аутентификации. Рассмотрены перспективы дальнейшего развития программного продукта.

Система аутентификации, двухфакторная аутентификация, электронный ключ, одноразовый пароль, цифровой сертификат, sms-канал

Проблема аутентификации в различных своих проявлениях стоит перед человечеством с давних времен, однако в настоящее время она приобрела исключительную актуальность. Это связано с глобальной информатизацией современного общества: информационные технологии пронизывают буквально все сферы человеческой деятельности. Основными приоритетами создаваемых в наши дни информационных систем являются надежность (в контексте безопасности) и удобство их эксплуатации, причем в первую очередь для конечного пользователя. Требование удобства, в свою очередь, предполагает проведение операций в информационной системе в удаленном режиме, что входит в компетенцию аутентификации и обусловливает высокую степень актуальности данной темы.

В [1]–[12] дан обзор методов аутентификации и их реализаций, а также различных исследований на данную тематику. По результатам данного обзора можно сопоставить основные методы аутентификации, применяемые в информационных системах для удаленного доступа (таблица).

Среди парольных методов наибольшего внимания заслуживают одноразовые пароли как самый надежный метод [1]. Многоразовые пароли и секретные вопросы обладают большей степенью удобства, однако в дальнейшем не рассматриваются ввиду крайне низкого уровня обеспечиваемой безопасности.

Перечисленные в таблице реализации аппаратного подхода к аутентификации характеризуются одинаковыми уровнями безопасности. При этом можно выделить подход на основе электронных ключей как наиболее удобный и дешевый.

Вид аутентификации	Метод аутентификации	Надежность	Удобство	Стоимость
Парольная	Многоразовый пароль	Средняя	Высокое	Высокая
	Одноразовый пароль	Высокая	Высокое	Высокая
	Секретный вопрос	Низкая	Высокое	Высокая
Аппаратная	Контактная память	Высокая	Высокое	Средняя
	Контактная смарт-карта	Высокая	Высокое	Средняя
	USB-ключ	Высокая	Высокое	Высокая
	RFID-система	Высокая	Высокое	Средняя
	Бесконтактная смарт-карта	Высокая	Высокое	Средняя

Из биометрических методов наиболее надежными являются подходы на основе идентификации по радужной оболочке и сетчатке глаза, однако ввиду низкой степени доступности подобных технологий данные методы в дальнейшем не рассматриваются. Остальные методы биометрической аутентификации, по сравнению с отмеченными ранее одноразовыми паролями и электронными ключами, обладают более низким уровнем надежности и по этой причине также не рассматриваются.

Таким образом, в качестве основы для разрабатываемого программного средства была выбрана модель двухфакторной аутентификации по электронным ключам и одноразовым паролям.

Постановка задачи. Для повышения безопасности при передаче данных по незащищенным каналам связи возникает необходимость разработки программного продукта, позволяющего проводить аутентификацию пользователей в облачном сервисе. Под облачным сервисом здесь и далее будет подразумеваться информационная система общего пользования, находящаяся на момент выполнения данной работы на стадии проектирования. Предметом деятельности защищаемого облачного сервиса является заключение различных экономических сделок, а также совершение товарно-коммерческих операций. Подобная тематика обусловливает основные требования, предъявляемые к разрабатываемому программному средству:

1. Обеспечение устойчивости к поддельной аутентификации.

2. Удобство в эксплуатации. Процесс аутентификации должен быть комфортным, в первую очередь для пользователей. В противном случае вся безопасность системы может быть сведена на «нет» пользователями, стремящимися облегчить прохождение процесса аутентификации.

3. Бюджетная окупаемость разработки и эксплуатации программного продукта.

4. Гибкость, т. е. возможность модификации системы под какие-либо нужды заменой ее составляющих (например, замена методов аутентификации и их реализаций или же замена криптографических алгоритмов).

Для достижения поставленной цели требуется разработать подход, позволяющий осуществлять процедуру двухфакторной аутентификации в виде клиент-серверного приложения.

Выбор архитектуры программного средства. В качестве основы для системы аутентификации была выбрана двухфакторная модель, представляющая собой разумный компромисс между удобством и надежностью [12]. Под надежностью здесь и далее понимается устойчивость к поддельной аутентификации. Исходя из этого, требуется выбрать 2 метода аутентификации из групп, различных по фактору, с учетом надежности. Из рассмотренных ранее механизмов аутентификации были выбраны одноразовые пароли и электронные ключи. Относительно одноразовых паролей стоит отметить, что данный метод обладает множеством реализаций. Одноразовые пароли могут быть переданы пользователю посредством электронных токенов – специальных устройств, генерирующих пароли и выводящих их на дисплей, или с помощью мобильных устройств (телефонов), где пароль может, как в случае с электронным токеном, генерироваться на устройстве и выводиться на экран либо же генерироваться на сервере и приниматься по SMS-каналу. Не стоит забывать и о подходе на основе бумажных или пластиковых носителей, когда пользователю передается список заранее сгенерированных аутентификационных кодов. Из перечисленных реализаций систем на основе одноразовых паролей была выбрана передача паролей по SMS, и в результате была получена базовая архитектура системы аутентификации (рис. 1).

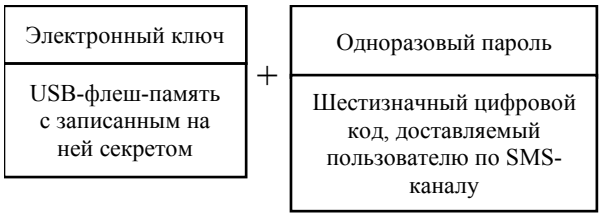

Рис. 1

Относительно непосредственной реализации электронного ключа отметим, что в разрабатываемой системе он представляет собой обычный usb-накопитель, который содержит цифровой сертификат пользователя, выступающий в роли секрета. При этом процесс аутентификации по электронному ключу заключается не только в проверке цифрового сертификата, но и в верификации носителя по дайджесту его аппаратных характеристик. Что касается одноразового пароля, то он представляет собой шестизначный цифровой код, генерируемый сервером и доставляемый пользователю по SMS-каналу при помощи GSM-модема.

Схема протекания процессов в системе аутентификации представлена на рис. 2, а диаграмма последовательности процесса аутентификации, которая отражает программное взаимодействие клиента и сервера, – на рис. 3. Рассмотрим схему работы системы аутентификации. Она состоит из клиентской части (пользователь, его рабочая станция, мобильный телефон и электронный ключ, содержащий цифровой сертификат пользователя и имеющий некоторые аппаратные характеристики) и серверной (непосредственно сам сервер, его подсистема сертификации, база данных, а также подсистема отправки SMS). Каждое действие в системе характеризуется литералом (буквенным сокращением, см. схему) процесса, в рамках которого оно выполняется, а также числом – номером шага. На данный момент в системе определено 3 процесса: настройка подсистемы сертификации, регистрация пользователя и непосредственно сама аутентификация пользователя.

Настройка подсистемы сертификации. Сервер создает собственный удостоверяющий центр (Н1), в котором в качестве корневого сертификата используется самоподписанный цифровой сертификат (Н2), выдаваемый серверу (Н3).

Регистрация пользователя инициируется обращением пользователя в центр сертификации (Р1), где происходит создание сертификата пользователя, а также подпись этого сертификата серверным (Р2). После этого пользователю выдается его цифровой сертификат на электронном ключе (Р3), а также сертификат сервера (Р4).

Наиболее сложным процессом является *аутентификация*. Пользователь вставляет свой электронный ключ (А1) и запускает приложение (А2). Далее между машиной клиента и сервером

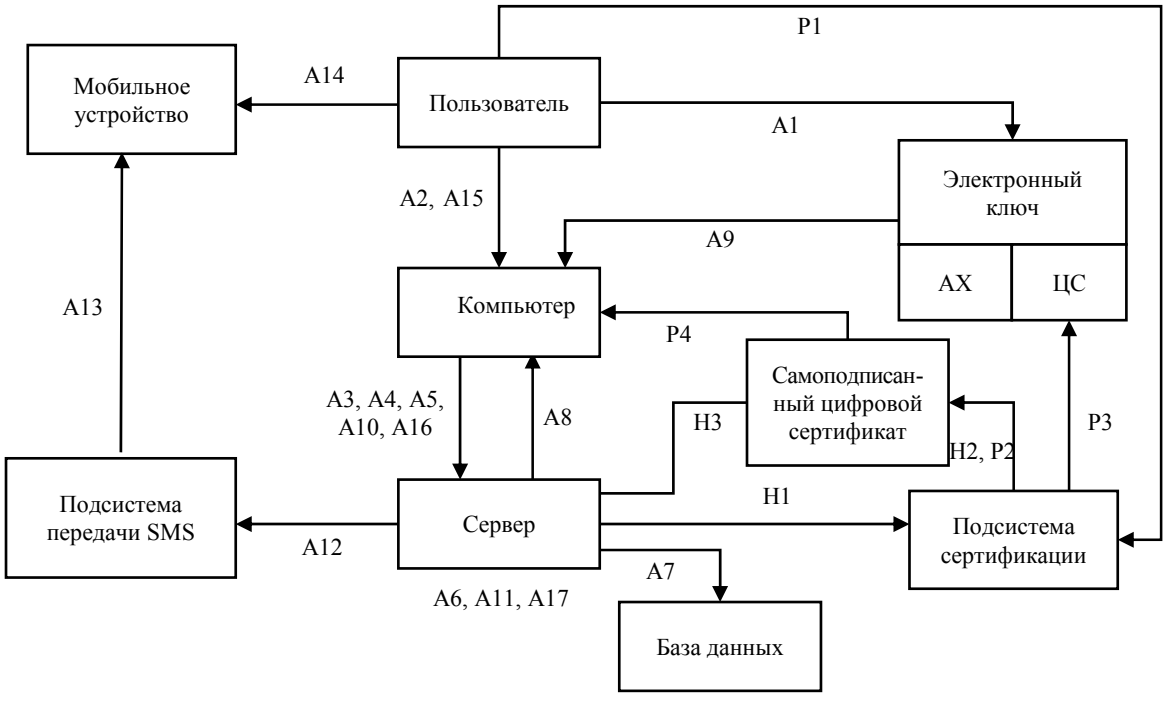

Рис. 2

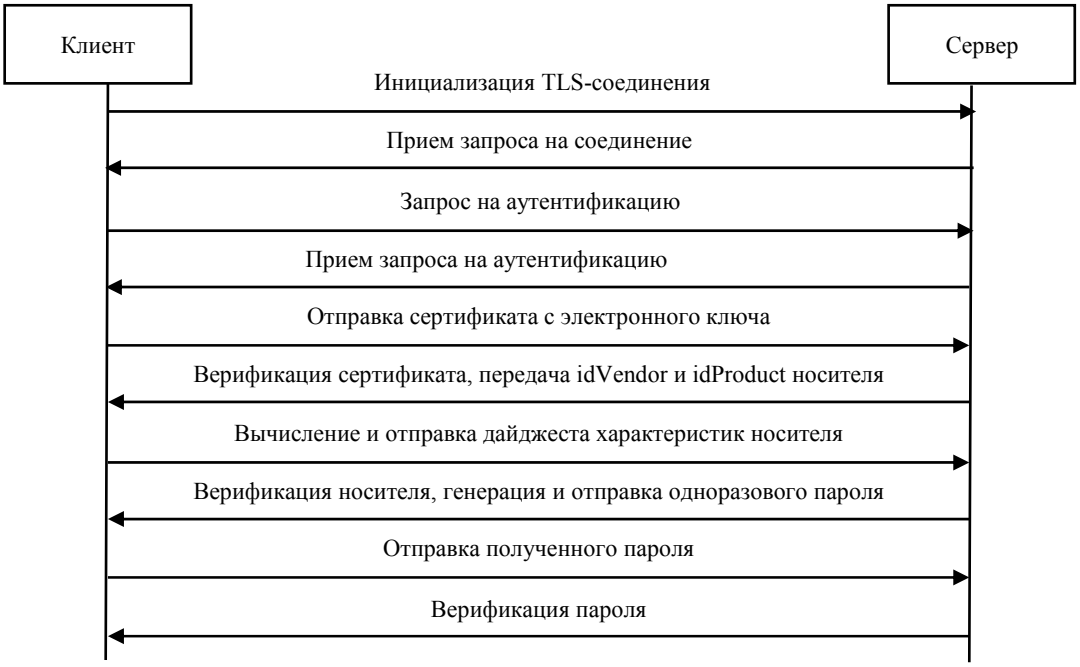

Рис. 3

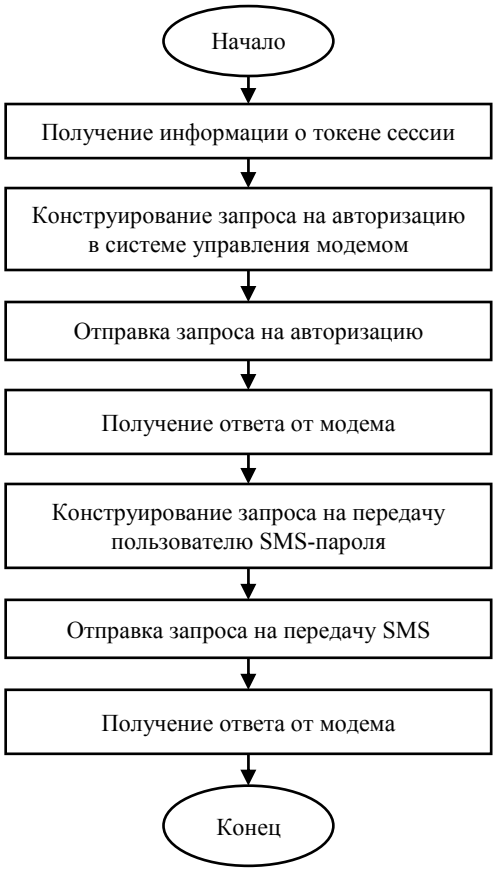

Рис. 4

Рис. 5

устанавливается TLS-соединение (А3), передается запрос на аутентификацию (А4) и цифровой сертификат пользователя (А5). Сервер проверяет сертификат пользователя (А6) и, если сертификат валиден, берет из базы данных его номер телефона, эталонное значение дайджеста аппаратных характеристик электронного ключа, а также код производителя и код продукта электронного клю-

ча (A7). Эти коды передаются пользователю (A8) и используются им для нахождения дайджеста аппаратных характеристик (A9). Полученная информация передается на сервер (A10), где проходит проверку (A11). Если дайджест соответствует эталонному значению, сервер генерирует одноразовый пароль (A12) и отправляет его пользователю (A13) по указанному в базе данных номеру телефона. У пользователя есть 60 с, чтобы получить (A14), ввести (A15) и отправить (A16) одноразовый пароль. Полученный сервером пароль сравнивается с отправленным, на основании чего принимается решение об аутентификации (A17).

Более подробно рассмотреть технические аспекты программного средства позволяют блок-схемы алгоритмов для серверной (основной процесс – рис. 4, функция send_sms – рис. 5, функция auth – рис. 6) и клиентской (рис. 7) частей.

Для разработки и функционирования системы в качестве серверных инструментов использовалась ОС Ubuntu Server версии 16.04, интерпретатор Python версии 3.6.3, система управления базами данных PostgreSQL версии 9.5, самоподписанный цифровой сертификат, а также 3G-модем Huawei e8231. Клиентская часть реализовывалась с использованием ОС Windows, интерпретатора Python 3, usb-носителя с записанным на нем цифровым сертификатом и мобильным устройством для приема SMS-сообщений.

Реализация. Процесс аутентификации начинается при запуске приложения и протекает в автоматическом режиме. При этом возможны различные сценарии протекания процесса аутентификации. В приведенном ниже листинге проиллюстрирована ситуация, в которой пользователь успешно проходит процедуру аутентификации, от лица клиента:

```
   Connected!
   Send: b'AUTH!-!-'
   Received: b'C_OK'
   Send: b'----BEGIN CERTIFICATE-----
\nMIIFiDCCA3ACAQMwDQYJKo2IhvcNA…
   Received: b'C_OK'
   Send: b'C_OK!-!-'
   Received: b'idv=5118idp=15872'
   idv=5118idp=15872
   5118 15872
   Send:
b'3395e369ddef58addeca22d98cc11920c76
b50bad07e635f10f70dc55…
   Received: b'C_OK'
   Please, enter the password, which
you received via SMS
   824529
   Received: b'C_OK'
   p OK:
   Process finished with exit code 0
```

Если пользователь не успевает ввести пароль или вводит неправильный, на экран выводится сообщение об ошибке и работа программы прекращается. При отсутствии электронного ключа или сертификата на нем программа ведет себя аналогичным образом.

Анализ безопасности и дальнейшие перспективы развития. В рамках анализа безопасности системы аутентификации оценивалась вычислительная сложность возможной атаки. Для того чтобы взломать систему, необходимо провести атаку на цифровой сертификат и атаку на одноразовый пароль. Атака на цифровой сертификат может быть осуществлена либо через вычисление закрытого ключа сервера, либо через нахождение коллизий хеш-функции. В цифровых сертификатах разработанной системы используется алгоритм шифрования RSA с длиной ключа 4096 бит и хеш-алгоритм SHA-512. Рассчитаем сложность наиболее эффективной атаки на RSA для чисел длиной более 110 знаков (общий метод решета числового поля) как

$$\exp\left(\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}\right).$$

В численном выражении сложность для 4096-битного ключа (n) составляет приблизительно $1.05 \cdot 10^{47}$ операций. Применительно к криптостойкости SHA-512 минимальная сложность «атаки дней рождений» на данную хеш-функцию может быть оценена как $2^{\frac{n}{2}}$ и составляет $2^{\frac{512}{2}} = 1.16 \cdot 10^{77}$. При этом данная атака направлена лишь на нахождение случайной коллизии хеш-функции, гарантированно предоставить искомую коллизию не позволяет даже полный перебор всех значений хеш-функции. Проведение любой из перечисленных атак является вычислительно трудной задачей, поэтому подделка цифрового сертификата, с учетом развития современной техники, также труднодостижима.

Что касается одноразовых паролей, то с учетом того, что после каждой неудачной попытки ввода пароля пользователю высылается новый, в силу длины пароля и его алфавита вероятность угадать пароль равна 10^{-6}, и соответственно, сложность атаки на пароль равна 10^6. Отметим, что данный метод крайне небрежен, так как подразумевает получение атакуемым пользователем

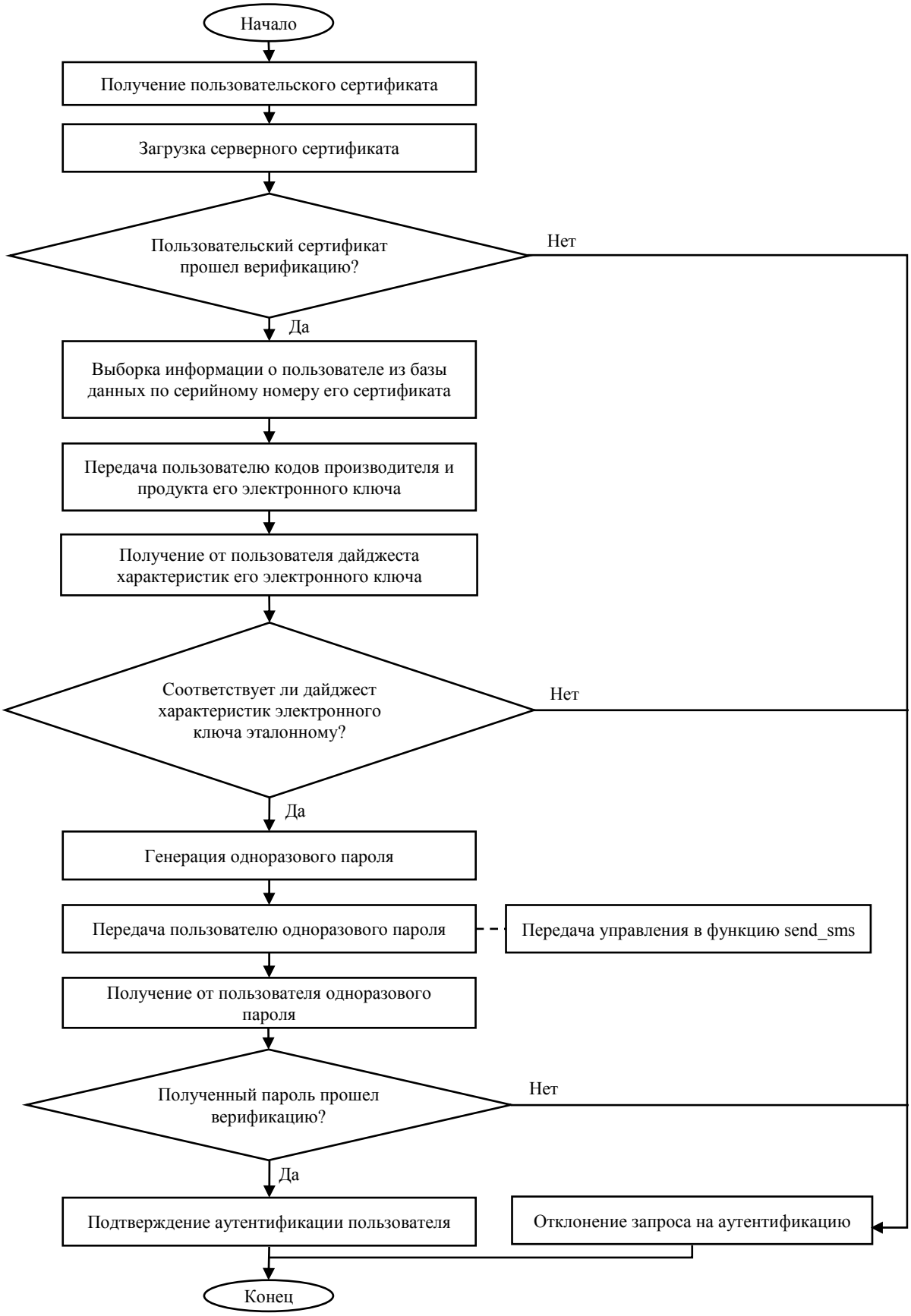
Начало
Получение пользовательского сертификата
Загрузка серверного сертификата
Пользовательский сертификат прошел верификацию?
Нет
Да
Выборка информации о пользователе из базы данных по серийному номеру его сертификата
Передача пользователю кодов производителя и продукта его электронного ключа
Получение от пользователя дайджеста характеристик его электронного ключа
Соответствует ли дайджест характеристик электронного ключа эталонному?
Нет
Да
Генерация одноразового пароля
Передача пользователю одноразового пароля
Передача управления в функцию send_sms
Получение от пользователя одноразового пароля
Полученный пароль прошел верификацию?
Нет
Да
Подтверждение аутентификации пользователя
Отклонение запроса на аутентификацию
Конец

Рис. 6

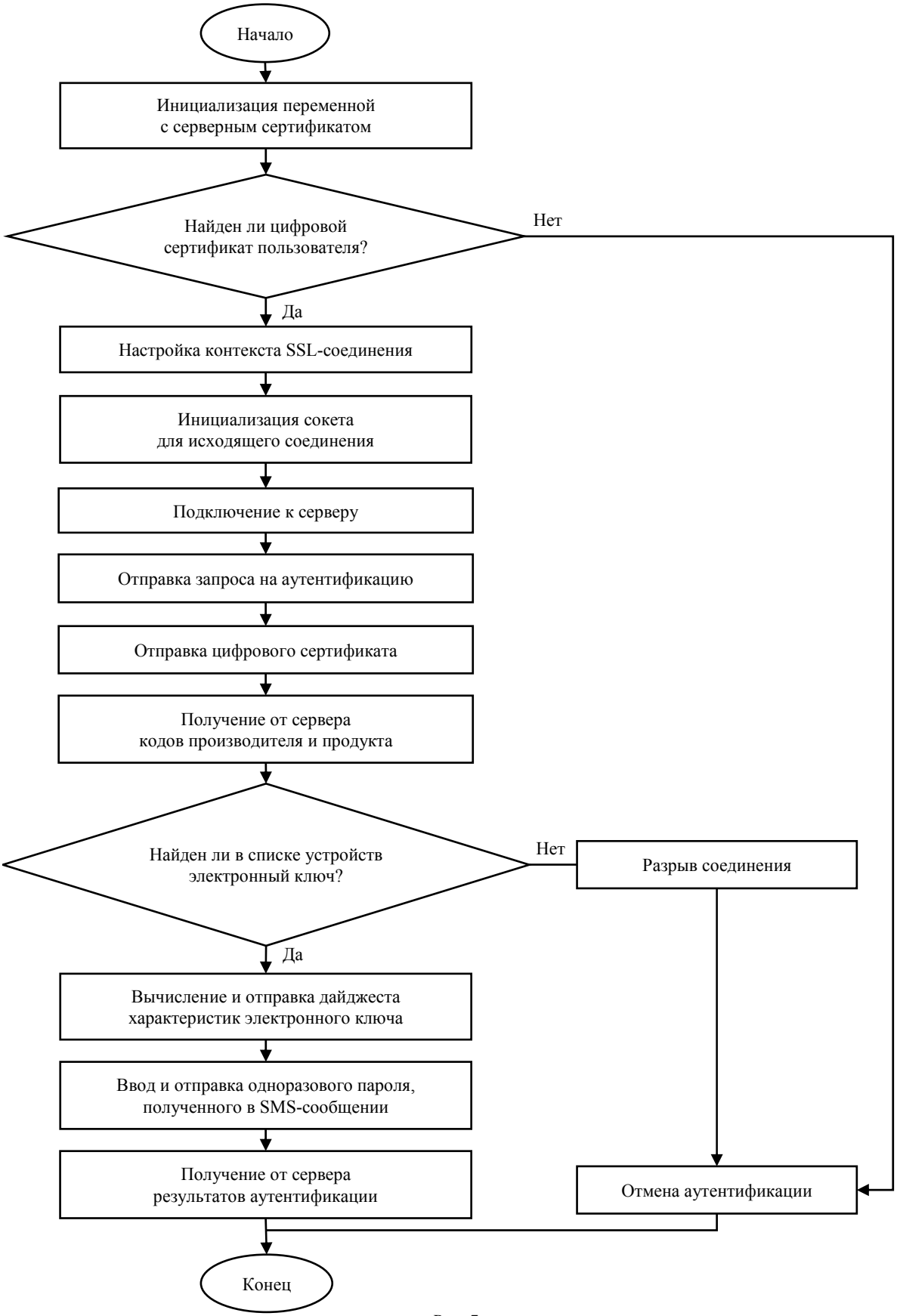
Начало
Инициализация переменной с серверным сертификатом
Найден ли цифровой сертификат пользователя?
Нет
Да
Настройка контекста SSL-соединения
Инициализация сокета для исходящего соединения
Подключение к серверу
Отправка запроса на аутентификацию
Отправка цифрового сертификата
Получение от сервера кодов производителя и продукта
Найден ли в списке устройств электронный ключ?
Нет
Разрыв соединения
Да
Вычисление и отправка дайджеста характеристик электронного ключа
Ввод и отправка одноразового пароля, полученного в SMS-сообщении
Получение от сервера результатов аутентификации
Отмена аутентификации
Конец

Рис. 7

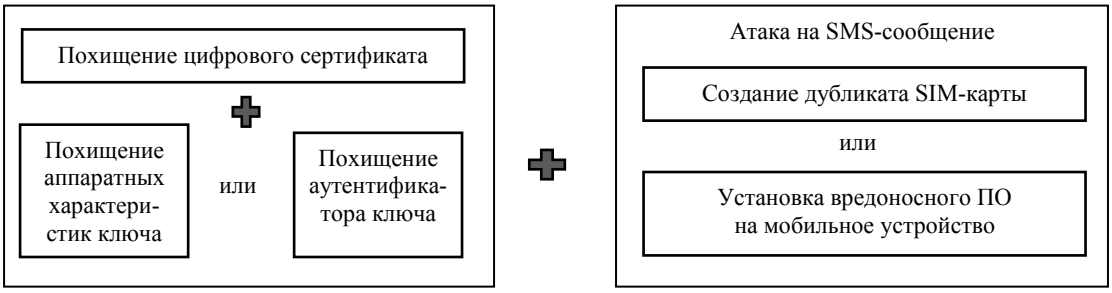

Рис. 8

SMS-сообщений с одноразовыми паролями. Атакуемый пользователь может заметить такого рода подозрительную активность и принять соответствующие меры (например, заморозить свой аккаунт и запросить новый набор аутентификаторов).

Оценивая быстродействие полученного решения, стоит отметить, что временные затраты на выполнение основной части программы, представляющей отрезок от установки соединения между клиентом и сервером до отправки одноразового пароля пользователю включительно, в среднем составляют 264 мс. Данный результат был получен при тестировании программного комплекса на виртуальной машине с одноядерным процессором частотой 3.0 ГГц. Клиентский хост при этом находился на локальной машине, поэтому полученная цифра не учитывает возможные задержки, возникающие в условиях настоящего интернет-соединения. Однако, если принять значение пинга в среднем равным 60 мс, время выполнения основной части программы будет оцениваться в районе 500 мс, что представляется достаточно быстрым для подобных систем аутентификации.

Полученное в результате разработки программное средство обладает рядом достоинств. На основании оценки сложности атаки было определено, что оно обеспечивает достаточный уровень безопасности. Кроме того, выполнено условие бюджетной окупаемости: затраты на эксплуатацию при правильном выборе SMS-тарифа (в среднем, около 60 к. за SMS) представляются приемлемыми. При этом предложенное программное решение также обладает высоким быстродействием и удобно в эксплуатации. Кроме того, архитектура системы аутентификации позволяет заменять используемые криптопримитивы и реализации методов аутентификации, что обусловливает ее гибкость.

Безусловно, у разработанной системы имеются и слабые места. Анализ работы программного средства показал, что взломать систему можно лишь посредством проведения комплексной атаки (рис. 8), состоящей из следующих фаз:

– похищения цифрового сертификата пользователя;

– похищения аутентификатора электронного ключа или его подделки;

– создания дубликата SIM-карты пользователя или установки вредоносного программного обеспечения на его мобильное устройство.

Однако вероятность подобной атаки представляется весьма низкой ввиду сложности проведения упомянутых мероприятий. Устраивать подобную атаку будет целесообразно, если затраты на ее проведение с высокой долей вероятности не превысят полученную выгоду.

Несмотря на это, возможность проведения упомянутой атаки представляет одну из актуальных проблем разработанной системы аутентификации. В связи с этим необходимо рассмотреть решение данной проблемы. Для этого заменим самоподписанный сертификат для сервера на доверенный, а электронный ключ в нынешнем виде на криптографический токен с неизвлекаемым секретом (рис. 9, 10).

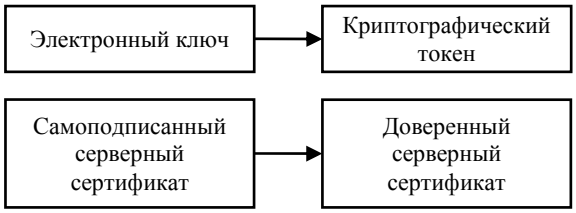

Рис. 9

Данное решение обладает рядом неоспоримых достоинств. Как уже отмечалось, использование доверенного сертификата в качестве серверного позволяет исключить возможность атаки «человек посредине». Кроме того, подобное решение так или иначе позволяет включить в систему возможность удаленной регистрации пользователей (при текущей конфигурации системы регистрация пользователей и передача электронного ключа должны происходить очно).

Внедрение процесса удаленной регистрации позволит повысить уровень удобства пользования системой, что должно положительно сказаться на динамике роста пользователей ИС в целом. В связи с этим удаленная регистрация является одним из ключевых аспектов дальнейшего развития системы аутентификации.

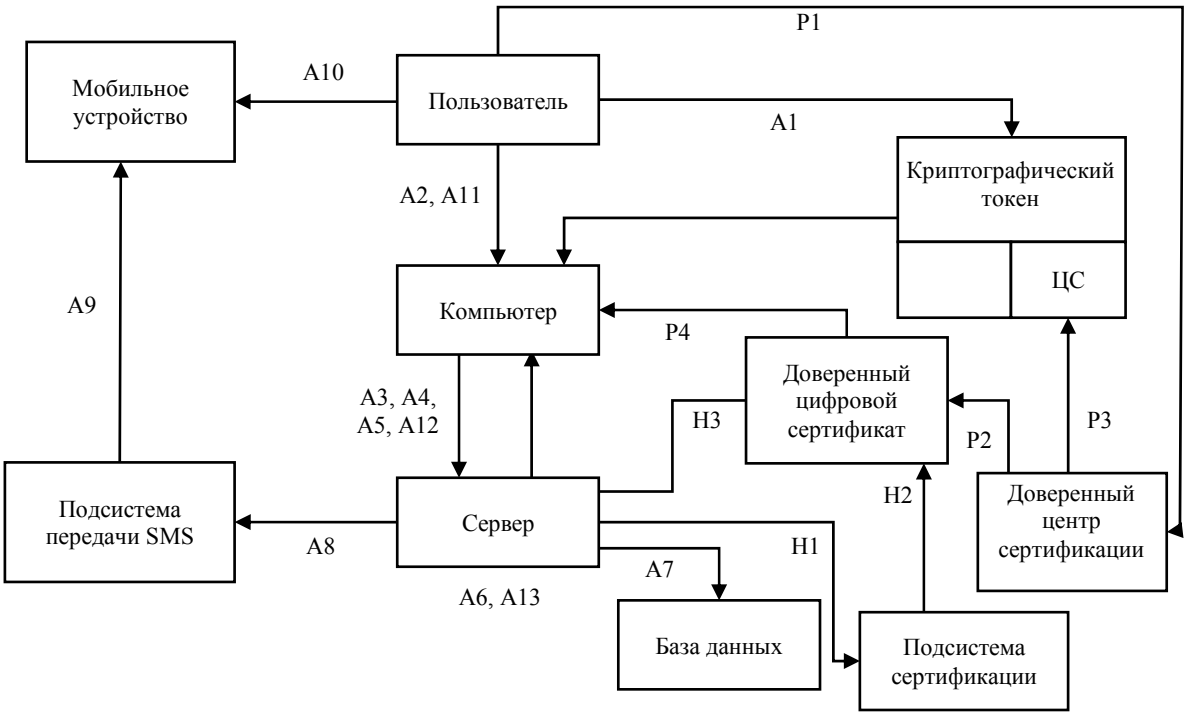

Рис. 10

В свою очередь, использование криптографического токена в качестве электронного ключа позволяет почти полностью исключить возможность компрометации пользовательского секрета (она становится возможной только в случае непосредственной кражи злоумышленником самого электронного ключа). Данное обстоятельство практически исключает проведение описанной ранее комплексной атаки – теперь она возможна только при физическом доступе к аутентификаторам жертвы, что является крайне маловероятным сценарием.

Таким образом, использование предложенной архитектуры в качестве базовой позволит почти полностью исключить вероятность взлома системы, делая ее практически неуязвимой. Однако внедрение данной архитектуры требует финансовых затрат на изготовление криптографических токенов и доверенных сертификатов. Это послужило ключевой причиной для реализации системы аутентификации в текущем виде и утверждения предложенной улучшенной архитектуры в рамках основного вектора дальнейшего развития программного продукта.

Что касается применимости системы, важно отметить, что благодаря высокому уровню обеспечиваемой безопасности, удобства и гибкости полученное программное средство может быть использовано для повышения безопасности доступа пользователей не только к защищаемой информационной системе, но и ко многим другим сервисам.

СПИСОК ЛИТЕРАТУРЫ

1. Классификация механизмов аутентификации пользователей и их обзор. URL: https://habrahabr.ru/post/177551/ (дата обращения 19.04.2018).

2. Косенко О. А., Широков Д. А. Анализ методов аутентификации пользователей // Тр. 11-й Междунар. молодежной науч.-техн. конф. «Современные проблемы радиотехники и телекоммуникаций "РТ-2015"» / Севастопольский гос. ун-т. Севастополь, 2015. С. 200–201.

3. Нифталиев С. Е. Двухфакторная аутентификация как инструмент информационной безопасности // Перспективы развития информационных технологий: тр. Всерос. молодежной науч.-практ. конф., 2014 г. / КузГТУ. Кемерово, 2014. С. 266–267.

4. Шафер А. Е. Двухфакторная аутентификация с использованием СМС // Вестн. Пермского ун-та. Сер.: Математика. Механика. Информатика. 2015. Т. 28, № 1. С. 79–85.

5. Вишняков В. А., Гондаг Саз М. М. Модели и средства аутентификации пользователей в корпоративных системах управления и облачных вычислениях // Докл. БГУИР. 2016. №3 (97). С 111–114.

6. Рацеев С. М., Череватенко О. И. Об оптимальных кодах аутентификации на основе конечных полей // Науч. ведомости БелГУ. Сер.: Математика. Физика. 2017. № 13 (262). С. 38–41.

7. Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication Procedia / J. Gualdoni, A. Kurtz, I. Myzyri, M. Wheeler, S. Rizvi // Computer Science. 2017. № 114. P. 93–99.

8. THRIVE: threshold homomorphic encryption based secure and privacy preserving biometric verification system (2015) / C. Karabat, M. S. Kiraz, H. Erdogan, E. Savas // Eurasip J. on Advances in Signal Proc. 2015. № 71. P. 1–18.

9. RFC 6238. TOTP: Time-Based One-Time Password Algorithm. URL: https://tools.ietf.org/html/rfc6238 (дата обращения 20.04.2018).

10. RFC 4226. HOTP: An HMAC-Based One-Time Password Algorithm. URL: https://tools.ietf.org/html/rfc4226 (дата обращения 20.04.2018).

11. ГОСТ Р 51241–2008. Средства и системы контроля и управления доступом. URL: http://docs.cntd.ru/document/1200071688 (дата обращения 20.04.2018).

12. Многофакторная аутентификация – лучше меньше, да лучше. URL: http://www.itsec.ru/articles2/Oborandteh/mnogofaktornaya-autentifikatsiya-luchshe-menshe--da-luchshe (дата обращения 20.04.2018).

V. D. Sergeev
Saint Petersburg Electrotechnical University «LETI»

R. R. Fatkieva
Saint Petersburg University for Informatics and Automation of the Russian Academy of Sciences

METHOD OF TWO-FACTOR AUTHENTICATION IN A CLOUD SERVICE

Existing authentication methods are reviewed, the comparative analysis of them is carried out. Based on the specifics of the protected system, a number of requirements for the authentication mechanism being developed are defined. Two-factor authentication method with electronic key, which represents electronic carrier, obtaining some hardware characteristics that also act as an additional authentication factor, with a secret recorded on it, and one-time six-digit password, transmitted to the user's mobile device via an SMS-channel, is proposed. The selection and further configuration of the infrastructure for authentication system software implementation is carried out, and realization of obtained algorithm is held. Authentication system architecture, which is embodied in the form of a client-server application, is introduced. As a result, software solution, which increases the security of user access to the cloud service, is received. Two-factor authentication system improvement activities are proposed as a part of further optimization. The prospects for further development of the software product are considered.

Authentication system, two-factor authentication, dongle, one-time password, digital certificate, SMS-channel

УДК 629.7.058.4

С. А. Кудряков, Е. А. Рубцов
Санкт-Петербургский государственный университет гражданской авиации

С. А. Беляев, А. В. Экало
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Ю. Б. Остапченко
АО «НИЦ СПб ЭТУ»

Анализ линий различной протяженности для обеспечения управления, контроля и связи с беспилотными воздушными судами

Произведен анализ линий передачи данных для обеспечения управления, контроля и связи с беспилотными воздушными судами. Рассматриваются три вида линий: дальнего, среднего и ближнего радиуса действия. Для обеспечения дальней радиосвязи с БВС в настоящее время возможно применение только спутниковых линий. Для обеспечения линий среднего радиуса действия (на дальность прямой радиовидимости) рекомендуется применять средства диапазонов УВЧ и СВЧ, позволяющие передавать данные с большой скоростью и обмениваться информацией с быстролетящими БВС. В настоящее время разработано большое количество средств данных диапазонов как военного, так и гражданского назначения. Линии ближнего радиуса действия применяются для обмена информацией между БВС и станцией внешнего пилота, а также для обмена информацией между БВС. Этот тип линий предполагает большие скорости передачи: от десятков мегабит до гигабит в секунду и позволяет обмениваться фото- и видеоинформацией в реальном масштабе времени. Помимо радиолиний для ближней связи целесообразно применять инфракрасные системы, не создающие помех в радиоэфире.

Безопасность полетов, беспилотные воздушные суда, управление, контроль, связь, линия передачи данных

Наблюдаемое в настоящее время развитие беспилотной авиации имеет по большей части стихийный характер. Это приводит к возникновению множества проблем и противоречий. Часть их видна