УДК 681.3.06

С.П. Евсеев[1], В.Г. Абдуллаев[2], Ж.Ф. Агазаде[2], В.С. Аббасова[2]

[1] *Харьковский национальный экономический университет имени С. Кузнеца, Харьков*
[2] *Азербайджанский государственный университет нефти и промышленности, Баку*

УСОВЕРШЕНСТВОВАНИЕ МЕТОДА ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ МОДИФИЦИРОВАННЫХ КРИПТО-КОДОВЫХ СХЕМ

Рассмотрена классификация методов двухфакторной аутентификации, основные достоинства и недостатки методов. Предлагается схема двухфакторной аутентификации на основе SMS-сообщений с использованием модифицированной крипто-кодовой схемы Мак-Элиса и Нидеррайтера, методика оценки рисков использования методов двухфакторной аутентификации, рассмотрены практические алгоритмы построения несимметричных крипто-кодовых систем.

Ключевые слова: *двухфакторная аутентификация, модифицированная крипто-кодовая схема Мак-Элиса и Нидеррайтера.*

Введение и анализ литературы

Методы двухфакторной аутентификации получили в последнее десятилетие широкое применение в различных областях коммуникационных технологий, связанных в первую очередь, с вопросами идентификации и допуска субъекта до конфиденциальной информации. Им доверяет большое число компаний, среди которых организации из сферы высоких технологий, финансового и страхового секторов рынка, крупные банковские учреждения и предприятия госсектора, независимые экспертные организации, а также исследовательские фирмы [1].

Двухфакторная безопасность – термин, описывающий принципы и механизмы аутентификация, которая требует одновременного присутствия двух компонентов со стороны пользователя: “что-то, что вы знаете”, и “что-то, что вы имеете. Традиционные системы используют имя пользователя и пароль для аутентификации. Этот метод обеспечивает минимальный уровень безопасности, поскольку имена и пароли можно легко перехватить и даже иногда просто угадать. В случае двухфакторной аутентификации пароль также используется в роли компонента “что-то, что вы знаете”, тогда как в качестве компонента “что-то, что вы имеете” обычно выступает некое устройство, например, *токен*. Среди токенов можно выделить одноразовые пароли, синхронизированные по времени, и одноразовые пароли на основе математического алгоритма. Синхронизированные по времени одноразовые пароли постоянно и периодически меняются. Такие токены хранят в памяти количество секунд, прошедших с 1 января 1970 года, и отображают часть этого числа на дисплее.

Чтобы пользователь мог осуществить вход, между токеном клиента и сервером аутентификации должна существовать синхронизация. Главная проблема заключается в том, что со временем они способны рассинхронизироваться, однако некоторые системы, такие как SecurID компании RSA, дают возможность повторно синхронизировать токен с сервером путем ввода нескольких кодов доступа. Более того, многие из этих устройств не имеют сменных батарей, потому обладают ограниченным сроком службы [7, 10]. Другие технологии, использующие тот же принцип двухфакторности, могут выполняться в форме сертификатов. *Сертификат* – это цифровой ключ. Обычно он хранится на жестком диске компьютера в качестве компонента “что-то, что вы имеете” и необходим при входе в систему в дополнении к паре “имя пользователя – пароль”. Проблема такого решения – низкая защищенность, так как сертификат может быть легко украден [1, 2].

Перспективным направлением в автоматизированных банковских системах является использование технологий 3D Secure (Verified by VISA и MasterCard Secure Code) и Passwindow, которые позволяют значительно снизить риски при сетевых расчетах [3, 4]. Другим примером является программное обеспечение 2FA One, позволяющее обеспечить расширенную двухфакторную и сквозную (единый вход, SSO – Single sign-on) аутентификацию к корпоративным ресурсам, повышая информационную безопасность организации по сравнению с традиционными методами использования логина и пароля [2]. Однако, проведенный анализ в работах [3 – 5] данных технологий выявляет некоторые уязвимости, которые могут привести к серьезным потерям в критических системах. Таким образом актуальной технической задачей является совершенствование методов двухфакторной аутентификации с учетом синергетической модели угроз, предложенной в работе [6].

Цели и задачи исследования

Целью статьи является рассмотрение классификации основных методов двухфакторной аутентифи-

кации и сравнительный анализ их применения, оценка основных угроз на основе синергетической модели угроз, построение методики оценки методов двухфакторной аутентификации. Усовершенствование метода двухфакторной аутентификации на основе SMS-сообщений на основе модифицированной крипто-кодовой системы (МККС) Мак-Элиса и несимметричной крипто-кодовой системы (НККС) Нидеррайтера, а также рассмотрение практических алгоритмов в предложенных крипто-кодовых системах.

Для достижения поставленной цели были поставлены следующие задачи:

– анализ основных методов двухфакторной аутентификации, оценка основных угроз на основе синергетической модели угроз;

– разработка схемы двухфакторной аутентификации на основе SMS-сообщений с использованием МККС Мак-Элиса и Нидеррайтера разработка практических алгоритмов шифрования и расшифрования данных;

– разработка методики оценки рисков методов двухфакторной аутентификации.

Результаты исследований

1. Анализ основных методов двухфакторной аутентификации, оценка основных угроз на основе синергетической модели угроз

Двухфакторная аутентификация или 2FA – это метод идентификации пользователя в каком-либо сервисе, где используются два различных типа аутентификационных данных. Введение дополнительного уровня безопасности обеспечивает более эффективную защиту аккаунта от несанкционированного доступа.

Двухфакторная аутентификация требует, чтобы пользователь имел два из трех типов идентификационных данных: “нечто, ему известное”, “нечто, у него имеющееся”, “нечто, ему присущее (биометрика)”.

Очевидно, что к первому пункту относятся различные пароли, ПИН-коды, секретные фразы и так далее, то есть что-то, что пользователь запоминает и вводит в систему при запросе.

Второй пункт – это *токен*, то есть компактное устройство, которое находится в собственности пользователя. Самые простые токены не требуют физического подключения к компьютеру – у них имеется дисплей, где отображается число, которое пользователь вводит в систему для осуществления входа – более сложные подключаются к компьютерам посредством USB и Bluetooth-интерфейсов. Сегодня в качестве токенов могут выступать смартфоны, потому что они стали неотъемлемой частью нашей жизни. В этом случае так называемый одноразовый пароль генерируется или с помощью специального приложения (например Google Authenticator), или приходит по SMS – это максимально простой и дружественный к пользователю метод, который некоторые эксперты оценивают как менее надежный [1, 7]. SMS PASSCODE® предлагает технологию, которая поможет преодолеть подобные трудности, сводя необходимость наличия чего-либо всего к одному универсальному устройству – мобильному телефону. Решение обеспечивает сеансовый процесс входа в систему, который проверяет имя пользователя и пароль и сверяют эту пару с одноразовым кодом, который отправляется пользователю на мобильный телефон. Другими словами, когда пользователь входит в систему, SMS PASSCODE® сначала проверяет имя пользователя и пароль, затем отправляет одноразовый код на мобильный телефон пользователя и, если пользователь вводит его правильно, разрешает доступ [1].

Таким образом, в основе методов двухфакторной аутентификации лежит на только традиционная связка “логин-пароль”, но и дополнительного уровня защиты – так называемого второго фактора, обладание которым нужно подтвердить для получения доступа к учётной записи или другим данным [8, 9].

Проведенный в работе [7] анализ выбора методов двухфакторной аутентификации показал, что 54,48 % респондентов используют двухфакторную SMS-аутентификацию в социальных сетях, и 69,42% при работе с финансами, однако, при решении рабочих вопросов предпочтение отдается токенам (45,36%).

Общая классификация методов двухфакторной аутентификации приведена на рис. 1.

Приведенный в работах [4, 8 – 11] анализ методов двухфакторной аутентификации показал следующие основные достоинства и недостатки:

Рис. 1. Классификация методов аутентификации

Достоинствами методов на основе SMS-оповещения являются генерация OTP-кодов при каждом входе и передача по дополнительному каналу, перехват логина и пароля пользователя по основному каналу не приведут злоумышленника к банковской информации клиента. Привязка ОТП-пароля к телефонному номеру клиента. Основными недостатками являются – отсутствие сигнала сотовой сети не позволяет использовать данные методы аутентификации, а использование только сотовых каналов приводит к "потере" двухфакторности аутентификации. Существует теоретическая вероятность подмены номера через услугу оператора или работников салонов связи.

Использование методов с приложениями-аутентификаторами (QR-коды) позволяет поддерживать несколько аккаунтов в одном аутентификаторе и формировать первичный ключ, нет необходимости использовать сотовые линии связи, генерация OTP-паролей на основе криптоалгоритмов. Основными недостатками являются – использование аутентификатора на том же устройстве, с которого осуществляется вход приводит к "потере" двухфакторности, доступ злоумышленника к первичному ключу пользователя приводит к взлому системы аутентификации.

Проверка входа с помощью мобильных приложений позволяет автоматизировать процесс аутентификации без участия пользователя на основе проверки личного ключа аутентификации на мобильном приложении. Основными недостатками являются – потеря/раскрытие личного ключа приводит к взлому системы аутентификации, использование аутентификатора на том же устройстве, с которого осуществляется вход приводит к "потере" двухфакторности.

Физические (или аппаратные) токены являются самым надёжным способом двухфакторной аутентификации. Чаще всего они представлены в виде USB-брелоков с собственным процессором, генерирующим криптографические ключи, которые автоматически вводятся при подключении к компьютеру. Преимуществами являются отсутствие использования дополнительных мобильных приложений, ПО, токены являются полностью независимыми девайсами. К недостаткам относятся – использование нескольких аккаунтов приводит к "связке" токенов, не поддерживается всеми приложениями.

Резервные ключи, являются запасным вариантом на случай утери/кражи смартфона, на который приходят одноразовые пароли или коды подтверждения. Потеря/кража резервных ключей приводит к разрушению конфиденциальности системы аутентификации.

Штрих-коды системы Passwindow обеспечивают уникальные статические изображения последовательности символов, генерируемых динамически сервером аутентификации без использования криптоалгоритмов. Любое вмешательство или подделка шаблона штрих-кода будет пассивно представлена пользователю в виде появления комбинаций в шаблоне, который не соответствуют ожиданиям. Существенным недостатком является возможность подбора уникального штрих-кода карточки, предложенного в работе [4].

Использование биометрии в качестве вторичного фактора идентификации осуществляется путем идентификации физических характеристик человека (отпечаток пальца, радужная оболочка глаза и т.п.). Достоинствами методов являются использование уникальных физиологических характеристик человека, отсутствие дополнительных мобильных приложений и ПО. Существенным недостатком является специфические требования к программно-аппаратным устройствам считывания биометрических данных пользователя.

Таким образом, в автоматизированных банковских системах, как правило, применяются системы двухфакторной аутентификации, основанные на одноразовых e-mail- или sms-паролях и различные типы токенов.

Оценка безопасности систем двухфакторной аутентификации. Анализ современных систем аутентификации показал, что их безопасность измеряется путем деления разности между стоимостью атак и выгоды для атакующего на стоимости защиты от них. Таким образом, дорогие, хотя и более безопасные методы, такие как криптографические PKI-устройства с собственными защищенными каналами связи, экранов и клавиатур оцениваются так низко по шкале безопасности, в то время как банковские системы все еще преимущественно опираются на самый дешевый и, казалось бы, наименее защищенных способ использования PIN-кодов и паролей. Общая стоимость и сложность развертывания таких устройств часто перевешивает пользу от их сверхвысокой безопасности. На основе синергетической модели угроз нарушения банковской безопасности, предложенной в работе [6] рассмотри основные типы угроз на системы двухфакторной аутентификации, общая классификация приведена на рис. 2.

Типичными методами атак в АБС являются [8]:

• *взламывание онлайновых баз данных* – похищение информации, хранящейся в торговых базах, данных;

• *человек посередине/фишинг* – третья сторона вмешивается и олицетворяет клиента и сервера, заставляя записывать и/или изменять сообщения друг друга;

• *атаки в области социнженирии* – клиентов обманывают с целью выведать их личные данные для последующей передачи хакеру;

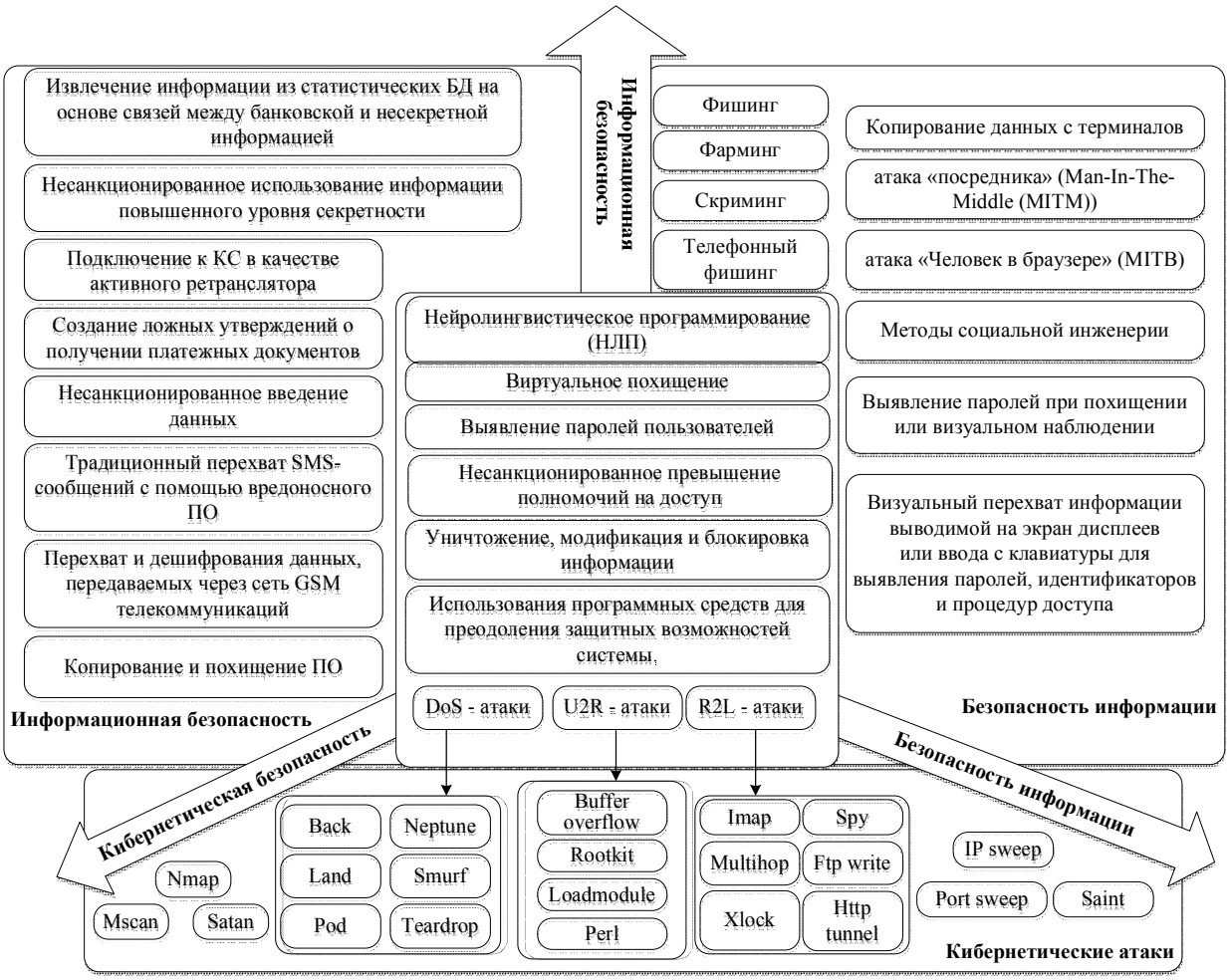


Рис. 2. Общая классификация угроз систем 2FA на основе синергетической модели угроз

• "*человек в браузере*" – вредоносная программа, установленная на компьютере жертвы, для сообщения о сетевой активности, нажатий клавиш, а также данных захваченных с экрана хакеру, позволяя ему перехватывать данные перевода средств, в которых средства могут быть невольно искажены путём изменения отображаемой информации в браузере пользователя;

• *атака полным перебором паролей пользователей* – сервер опрашивается со всеми возможными комбинациями паролей;

• *простая кража* – подробности об аутентификации записаны или на карточке могут быть физически приняты и скопированы;

• *наблюдение со спины* – злоумышленник может незаметно наблюдать, как пользователь вводит детали своей сделки.

Проведенный анализ угроз на основе синергетического подхода к оценке угроз показал, что злоумышленники на сегодняшний день используют комплексный подход к получению персональных данных пользователей, основанный на объединении методов социальной инженерии с традиционными методами маскарада и проникновения. Кроме этого используются и новые виды кибератак, позволяющие эффективно встраивать вредоносное ПО на мобильные средства связи, что в свою очередь приводит к снижению рентабельности методов двухфакторной аутентификации на основе SMS-сообщений и OTP-паролей в АБС. Таким образом, возникает необходимость использования дополнительных средств обеспечения конфиденциальности передачи информации в сотовых системах связи.

2. Разработка схемы двухфакторной аутентификации на основе SMS-сообщений с использованием МККС Мак-Элиса и Нидеррайтера, практических алгоритмов шифрования и расшифрования данных

Обозначение *SMS-систем или систем двухфакторной аутентификации на основе мобильных телефонов* является ошибочным, более точный термин – это "внеполосная" аутентификация. Тем не менее, с распространением GSM, смартфонов и планшетов подключенным к сети, даже это преимущество безопасности может быть утеряно, если аутентификация транзакции пользователя осуществляется на самом мобильном устройстве. Кроме того, рост нежелательного программного обеспечения для мобильных устройств теперь позволяет злоумышленнику получить доступ к кодам аутентифи-

кации, отправленных через SMS не только с помощью традиционного перехвата с помощью вредоносного ПО.

Проведенный анализ Интернет-атак на схемы двухфакторной аутентификации с использованием SMS-сообщений и достоинства крипто-кодовых схем позволяют усовершенствовать схему двухфакторной аутентификации с целью повышения уровня криптостойкости и достоверности формируемого аутентификатора.

Для этого банковская карточка (БК), должна хранить следующие элементы данных:

(1) *Индекс открытого ключа центра сертификации* – так как терминал может работать с несколькими центрами сертификации, эта величина специфицирует, какой из ключей необходимо использовать терминалу при работе с данной картой;

(2) *Сертификат открытого ключа эмитента* – подписывается соответствующим центром сертификации;

(3) *Сертификат открытого ключа БК* – подписывается эмитентом и формируется на основе МККС Мак-Элиса.

(4) Модуль и экспоненту открытого ключа эмитента.

(5) Модуль и экспоненту открытого ключа БК.

(6) Секретный ключ БК.

Терминал, поддерживающий схему двухфакторной аутентификации, должен хранить открытые ключи всех центров сертификации и ассоциированную информацию, относящуюся к каждому из ключей. Терминал должен также уметь выбирать соответствующие ключи на основе индекса (1) и некоторой специальной идентификационной информации.

Для поддержки двухфакторной аутентификации банковская карточка (БК) пользователя должна иметь свою собственную ключевую пару (открытый и секретный ключи аутентификатора). Открытый ключ БК хранится на БК в сертификате её открытого ключа. Каждый открытый ключ БК сертифицируется её эмитентом, а доверенный центр сертификации сертифицирует открытый ключ эмитента. Это означает, что для проверки аутентификатора карты терминалу вначале необходимо проверить два сертификата для того, чтобы восстановить и аутентифицировать открытый ключ БК, который затем применяется при проверке аутентификатора БК.

Процесс предлагаемой аутентификации состоит из четырех этапов:

(1) *Восстановление терминалом открытого ключа центра сертификации*. Терминал считывает индекс (1), идентифицирует и извлекает хранящиеся в нём модуль и экспоненту открытого ключа центра сертификации, и ассоциированную информацию, выбирает соответствующие алгоритмы.

(2) *Получение секретных мест в векторе ошибки от банка эмитента*. Формирование вектора ошибки путем введения пользователем кратности.

(3) *Формирование аутентификатора на основе использования МККС Мак-Элиса*. Получение кодового слова (аутентификатора) на основе использования крипто-кодовой схемы.

(4) *Проверка подлинности аутентификатора.* Нахождение кратности вектора ошибки и сравнение с полученным.

Структура предлагаемого метода двухфакторной аутентификации на основе ККС Мак-Элиса и Нидеррайтера представлена на рис. 3.

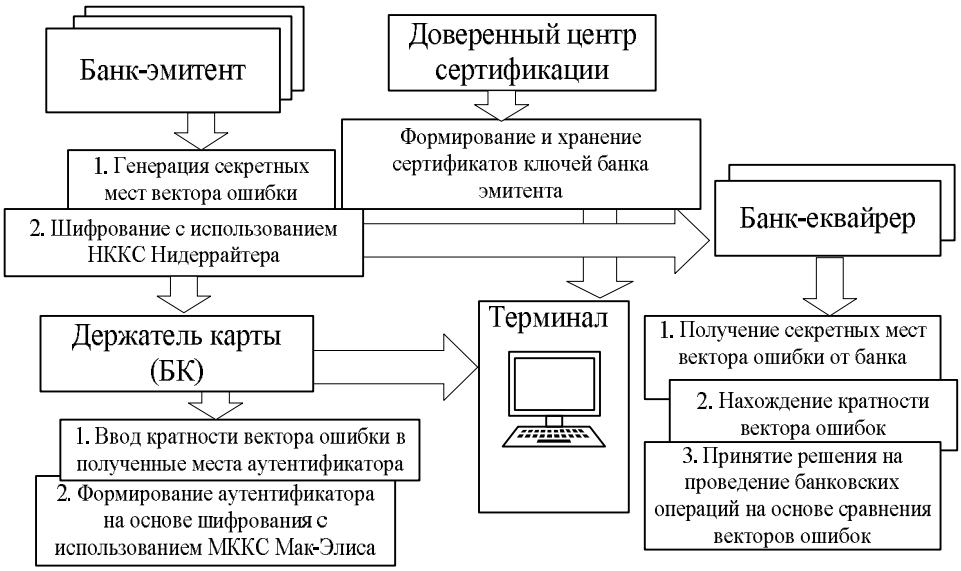


Рис. 3. Структура предлагаемого метода двухфакторной аутентификации на основе модифицированной крипто-кодовой системы Мак-Элиса и НККС Нидеррайтера

Существенным достоинством, на взгляд авторов, использования данной двухфакторной схемы аутентификации является обеспечение требуемых показателей криптостойкости передаваемых тран-

закций на основе использования несимметричных крипто-кодовых систем Мак-Элиса и Нидеррайтера, а также различные подходы в их построении в двух каналах связи: передача SMS-сообщения по сотовым каналам мобильной связи с использованием НККС Нидеррайтера (обеспечивается конфиденциальность OTP-пароля), и использование в цифровых каналах АБС МККС Мак-Элиса, где в качестве сеансового ключа используется значение полученного OTP-пароля. Использование сеансового ключа при каждой транзакции и упрощенный алгоритм раскодирования (в алгоритме Берлекемпа-Месси нет необходимости выполнять задачу локализации по процедуре Месси), возможность передачи по различным каналам связи, масштабируемость программного модуля путем изменения использования ККС Мак-Элиса и Нидеррайтера, в зависимости от уровня ошибок в используемых коммуникационных каналах АБС. Рассмотрим практические протоколы построения крипто-кодовых систем, используемых в протоколе двухфакторной аутентификации.

Наиболее простой и удобный способ модификации линейного блокового кода, не уменьшающий минимальное кодовое расстояние, состоит в укорочении его длины путем сокращения информационных символов [12 – 14]. Пусть $I = (I_1, I_2, \ldots, I_k)$ – информационный вектор (n, k, d) блокового кода. Выберем подмножество h информационных символов, $|h| = x$, $x \le ½ k$. Поместим в информационный вектор I в подмножество h нули, т. е. $I_i=0$, $\forall I_i \in h$. На остальных позициях вектора I поместим информационные символы. При кодировании информационного вектора символы множества h не участвуют (они нулевые) и их можно отбросить, а полученное кодовое слово будет короче на x кодовых символов. Для модификации (укорочения) эллиптических кодов будем использовать уменьшение набора точек кривой. Справедливо следующее утверждение [15].

Утверждение 1. Пусть EC – эллиптическая кривая над GF(q), g=g(EC) – род кривой, EC(GF(q)) – множество ее точек над конечным полем, N=EC(GF(q)) – их число. Пусть X и h – непересекающиеся подмножества точек, $X \cup h = EC(GF(q))$, $|h| = x$. Тогда укороченный эллиптический (n, k, d) код над GF(q), построенный через отображение вида $\varphi: X \to P^{k-1}$, связан характеристиками $k+d \ge n$, причем:

$$n = 2\sqrt{q} + q + 1 - x,$$

$$k \ge \alpha - x, \quad d \ge n - \alpha, \ \alpha = 3 \times \text{degF}., \qquad (1)$$

Утверждение 2. *Укороченный* эллиптический (n, k, d) код над GF(q), построенный через отображение вида $\varphi: X \to P^{r-1}$, связан характеристиками $k + d \ge n$, причем:

$$n = 2\sqrt{q} + q + 1 - x,$$

$$k \ge n - \alpha, \ d \ge \alpha, \ \alpha = 3 \times \text{degF}. \qquad (2)$$

Используя результат утверждений 1, 2 зададим теоретико-кодовую схему на модифицированных эллиптических кодах, построенную через отображение вида $\varphi: X \to P^{k-1}$ и $\varphi: X \to P^{r-1}$. Справедливы следующие утверждения.

Утверждение 3. Укороченный эллиптический (n, k, d) код над $GF(2^m)$, построенный через отображения вида $\varphi: X \to P^{k-1}$, определяет модифицированную теоретико-кодовую схему с параметрами:

$$l_{K+} = x \cdot \left\lceil \log_2 \left(2\sqrt{q} + q + 1 \right) \right\rceil; \qquad (3)$$

$$l_I = (\alpha - x) \cdot m; \qquad (4)$$

$$l_S = \left(2\sqrt{q} + q + 1 - x \right) \cdot m; \qquad (5)$$

$$R = (\alpha - x) / \left(2\sqrt{q} + q + 1 - x \right). \qquad (6)$$

Утверждение 4. Укороченный эллиптический (n, k, d) код над $GF(2^m)$, построенный через отображения вида $\varphi: X \to P^{r-1}$, определяет модифицированную теоретико-кодовую схему с параметрами:

– размерность секретного ключа определяется выражением (3), а размерность информационного вектора (в битах):

$$l_I = \left(2\sqrt{q} + q + 1 - \alpha \right) \cdot m; \qquad (7)$$

– размерность кодограммы определяет (5);

– относительная скорость передачи:

$$R = \left(2\sqrt{q} + q + 1 - \alpha \right) / \left(2\sqrt{q} + q + 1 - x \right). \qquad (8)$$

Рассмотрим практические алгоритмы формирования и расшифрования/раскодирования криптограммы/кодограммы в модифицированной несимметричной крипто-кодовой системе на основе ТКС Мак-Элиса на укороченных эллиптических кодах. На рис. 4 представлен алгоритм формирования криптограммы/кодограммы.

Алгоритм формирования кодограммы в модифицированной теоретико-кодовой схеме Мак-Элиса с укороченным модифицированным кодом зададим последовательностью следующих шагов:

Шаг 1. Зафиксируем конечное поле *GF(q)*. Зафиксируем эллиптическую кривую

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3$$

и набор ее точек $EC(GF(q)):(P_1, P_2, \ldots, P_N)$ над GF(q). Зафиксируем подмножество точек $h(GF(q)): (P_{x1}, P_{x2}, \ldots, P_{xx})$, $h \subseteq EC(GF(q))$, $|h|=x$ и храним его в секрете.

Шаг 2. Сформируем вектор инициализации $IV=EC–h_j$, h_j – информационные символы равные нулю, $|h| =1/2k$, т. е. $I_i = 0$, $\forall I_i \in h$;

Шаг 3. По введенному информационному вектору I сформируем кодовое слово c. Если (n, k, d) код над GF(q) задан своей порождающей матрицей, то $c=I \cdot G$.

Шаг 4. Сформируем случайный вектор ошибки e такой, что $w(e) \le t$, $t = \lfloor (d-1)/2 \rfloor$. Добавим сформированный вектор к кодовому слову, получим кодовое слово: $c^*=c+e$.

Шаг 5. Сформируем кодограмму, путем удаления (укорочения) символов вектора инициализации: $c_X^* = c^* - IV$.

Алгоритм раскодирования кодограмм в модифицированных теоретико-кодовых схемах на эллиптических кодах зададим последовательностью следующих шагов.

Шаг 1. Ввод кодограммы, подлежащей раскодированию. Ввод закрытого ключа – порождающей и/или проверочной матрицы эллиптического кода.

Шаг 2. Кодограмма – суть кодовое слово с ошибками эллиптического кода. Вес вектора ошибок $w(e) \le t$. Раскодируем кодограмму – находим вектор ошибок.

Шаг 3. Формируем искомый информационный вектор.

Предложенный алгоритм раскодирования в модифицированной несимметричной крипто-кодовой системе с использованием ТКС Мак-Элиса с укороченным модифицированным кодом представлен на рис. 5.

Проведем исследование энергетических затрат на программную реализацию крипто-кодовых средств защиты информации на основе ТКС Мак-Элиса на модифицированных (укороченных) эллиптических кодах.

Оценка энергетических затрат на программную реализацию предлагаемой системы Мак-Элиса. Для оценки временных и скоростных показателей принято использовать единицу измерения cpb, где cpb (cycles per byte) – число тактов процессора, которое необходимо потратить для обработки 1 байта входящей информации.

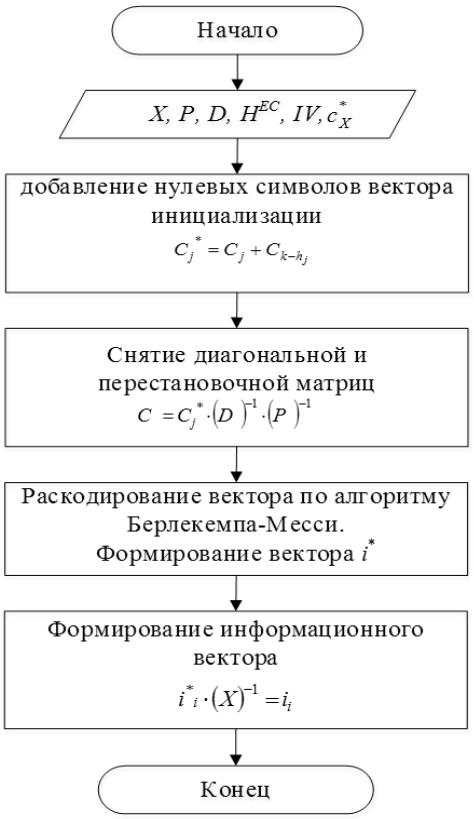
Рис. 4. Алгоритм формирования кодограммы в модифицированной НККС Мак-Элиса с укороченным модифицированным кодом

Сложность алгоритма вычислим по выражению

$$Per = Utl * CPU\_clock / Rate,$$

где Utl – утилизация ядра процессора (%); Rate – пропускная способность алгоритма (байт/сек).

В табл. 1 приведены результаты исследований зависимости длины кодовой последовательности алгеброгеометрического кода в ТКС Мак-Элиса и Нидеррайтера от количества тактов процессора на выполнение элементарных операций в программной реализации крипто-кодовых систем.



Этап 1. Установка параметров кода, ввод личного ключа и кодограммы

X – невырожденная $k \times k$ матрица над $GF(q)$,
P – перестановочная $n \times n$ матрица над $GF(q)$,
D – диагональная $n \times n$ матрица над $GF(q)$,
H^{EC} – проверочная $r \times n$ матрица эллиптического кода над $GF(q)$, a_i – набор коэффициентов многочлена кривой $a_1 \ldots a_6$,
IV – вектор инициализации, IV= $|h|$ =½ k – элементы сокращения

Этап 2. Раскодирование кодограммы

Рис. 5. Алгоритм в модифицированной НККС Мак-Элиса с укороченным модифицированным кодом

Таблица 1

Зависимость длины кодовой последовательности кода от количества тактов процессора

Длина кодовой последовательности		MacElis на укороченных кодах			MacElis		
		10	100	1000	10	100	1000
Кол-во вызовов функций элемент. операции	Чтение символа	10294397	28750457	76759874	11018042	30800328	80859933
	Сравнение строк	3406921	9246748	25478498	3663356	10199898	26364634
	Конкатенация строк	1705544	5045748	12379422	1834983	5125564	13415329
Сумма		15406862	43042953	114617794	16516381	46125790	120639896
Длительность выполн. функций* в тактах CPU	Чтение символа	295374	810478	2001167	297487	831609	2183218
	Сравнение строк	178814	531379	1248684	197821	550794	1423690
	Конкатенация строк	544990	1328114	3586486	544990	1522293	3984353
Сумма		1006781	2749548	7247488	1040298	2904696	7591261
Длительность выполнения** в мсек		0,52	1,37	3,4	0,55	1,53	4

*Примечание: * длительность 1000 операций в тактах процессора: чтение символа – 27 тактов, сравнение строк – 54 такта, конкатенация строк – 297 тактов; ** для расчета взят процессор с тактовой частотой 2 ГГц с учетом загрузки операционной системой 5 %*

В табл. 2 результаты исследований оценки временных и скоростных показателей процедур формирования и раскодирования информации в несимметричных крипто-кодовых системах на основе ТКС Мак-Элиса.

Проведенный анализ табл. 1, 2 позволяет сделать вывод о значительных энергетических затратах при реализации несимметричных крипто-кодовых систем в протоколах коммуникационных систем и технологий, что значительно затрудняет их использование.

Таблица 2

Оценка временных и скоростных показателей процедур преобразования информации

Показатели	Длина кодовой последовательности	Rate (байт/сек)	Утилизация ядра процессора (%)	Per (cpb)
Кол-во вызовов функций элемент. операций	100	46 125 790	56	61,5
	1000	120 639 896	56	62,0

Для устранения недостатка предлагается использовать МККС на основе использования модификации помехоустойчивых кодов, что обеспечивает снижение энергетических затрат и объемов ключевых данных пользователей за счет хранения данных о коэффициентах эллиптической кривой в аффинном пространстве для построения соответствующих матриц (закрытого и открытого ключей).

При проведении транзакций в АБС ОТР-пароль составляет четыре символа, поэтому для обеспечения стойкости метода двухфакторной аутентификации на основе МККС Мак-Элиса достаточно построение НККС в поле $GF(2^{6\text{-}7})$, что существенно уменьшает энергетические затраты на их реализацию, и позволяет использовать их в мобильных приложениях не нарушая основные протоколы передачи данных в сотовых каналах связи.

3. Разработка методики оценки рисков методов двухфакторной аутентификации.

Анализ рисков может быть выполнен с различной степенью детализации в зависимости от критичности ресурсов СУИБ / бизнес-процессов / банковских продуктов, известных уязвимостей и предыдущих инцидентов информационной безопасности. Методология оценки рисков может быть количественной или качественной, или их комбинацией. На практике качественная оценка часто используется в первую очередь для определения общего уровня риска и определения основных рисков. Далее может возникнуть необходимость проведения более специфического или количественного анализа по основным рискам. Количественная оценка рисков является более сложной и требует больше времени и ресурсов. Однако такая оценка будет очень полезной в случаях, когда решение по обработке рисков будет зависеть от стоимости мер безопасности, которые могут быть большими, чем финансовые потери инцидента информационной безопасности [16]. Введем следующие определения [17]:

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации банковской системы (ОБС); находящаяся в распоряжении организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме;

Источник угрозы информационной безопасности; источник угрозы ИБ – объект или субъект, реализующий угрозы ИБ путем воздействия на объекты среды информационных активов ОБС;

Модель угроз информационной безопасности; модель угроз ИБ – описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба;

Объект среды информационного актива – материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.);

Оценка риска нарушения информационной безопасности: систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения банковской безопасности (ББ), связанных с использованием информационных активов ОБС на всех стадиях их жизненного цикла.

Для оценки рисков нарушения ББ на основе использования методов двухфакторной аутентификации предварительно определяются и документально оформляются:

– полный перечень типов информационных активов, входящих в область оценки;

– полный перечень типов объектов среды, соответствующих каждому из типов информационных активов области оценки;

– модель угроз ББ, описывающую угрозы ББ для всех выделенных в ОБС типов объектов среды на всех уровнях иерархии информационной инфраструктуры ОБС.

Риск нарушения ББ определяется на основании качественных оценок:

– *степени возможности реализации угроз* Б*Б* (СВР угроз ББ) выявленными и (или) предполагаемыми источниками угроз ББ в результате их воздействия на объекты среды рассматриваемых типов информационных активов;

– *степени тяжести последствий от потери свойств ББ* для рассматриваемых типов информационных активов (СТП нарушения ББ).

Оценка СВР угроз ББ и СТП нарушения ББ базируется на экспертной оценке, выполняемой сотрудниками службы ББ ОБС с привлечением сотрудников подразделений информатизации [17]. Риски нарушения ББ могут быть оценены в количественной (денежной) форме.

Для оценки рисков нарушения ББ на основе использования методов двухфакторной аутентификации в количественной форме проведем на основании количественных оценок:

– *степени возможности реализации угроз ББ* (СВР угроз ББ), выраженной в количественной форме (%) ($СВР_{кол}$ угроз ББ);

– *степени тяжести последствий от потери свойств ББ* (СТП нарушения ББ), выраженной в количественной форме ($СТП_{кол}$ нарушения ББ).

Для выполнения оценки рисков определим шкалу для различных параметров: оценки величины последствий реализации угрозы на сервисы безопасности (целостность, конфиденциальность, доступность, наблюдаемость), оценки вероятности реализации угрозы. Общий уровень оценки величины последствий реализации каждой угрозы на сервисы безопасности определяется как максимальная величина из

отдельных оценок воздействия на целостность, конфиденциальность, доступность, наблюдаемость.

В табл. 3, 5 – 8 приведены шкалы для оценки рисков сервисов безопасности (целостность, конфиденциальность, доступность, наблюдаемость) [16, 17].

Данные на основании которых проводится оценка $СВР_{кол}$ угроз ББ, и ее результаты документируются, для чего рекомендуется использовать примерную форму (табл. 4) документирования данных и результатов оценки $СВР_{кол}$ угроз ББ

Таблица 3

Оценка вероятности реализации угроз $СВР_{кол}$ угроз ББ

СВР угроз ББ	Описание	$СВР_{кол}$ угроз ББ
нереализуемая	Возникновение инцидента практически невозможно	0 %
минимальная	Возникновение инцидента маловероятно (не чаще 1 раза в 1 год)	от 1 % до 20 %
средняя	Возникновение инцидента вероятно до 1 раза в 3 месяца	от 21 % до 50 %
высокая	Возникновение инцидента вероятно до 1 раза в неделю	от 51 % до 100 %
критическая	Возникновение инцидента вероятно до 1 раза в сутки	100 %

Таблица 4

Примерная форма документирования данных и результатов оценки $СВР_{кол}$ угроз ББ при использовании методов двухфакторной аутентификации (на примере заполнения: тип информационного актива – OTP-пароль; свойство ББ – конфиденциальность; способ реализации угрозы – "несанкционированное копирование" (НСК); тип объекта среды – сеансовый ключ пользователя; источник угроз – инсайдер, злоумышленник)

Тип инф. актива	Тип объекта среды	Источник угроз ББ	Свойства ББ типа инф. актива	Способ реализации угроз ББ	Априорные защитные меры	Прочие данные для определения $СВР_{кол}$ угроз ББ	Оценка $СВР_{кол}$ угроз ББ
сеансовый ключ пользователя	ключевые данные транзакции	инсайдер	конфиденциальность	НСК	Проведение кадровой политики, мониторинг и протоколирование доступа	Пользователь, имеющий право доступа к к OTP-паролям	56%
		…					
	ключевые данные транзакции	злоумышленник	конфиденциальность	НСК	контроль и протоколирование доступа. Организация программной защиты	нет данных	5%

Таблица 5

Оценка вероятности реализации угроз $СТП_{кол}$ нарушения ББ (влияние на целостность)

СТП нарушения ББ	Описание	$СТП_{кол}$ нарушения ББ
нереализуемая	Практически не приводит к последствиям с финансовыми потерями	до 0,01 % от величины капитала ОБС
минимальная	Приводит к значительным финансовым потерям и имеет незначительное влияние на репутацию банка	от 0,01 % до 0,5 % от величины капитала ОБС
средняя	Приводит к значительным финансовым потерям и имеет значительное влияние на репутацию банка	от 0,5 % до 1,5 % от величины капитала ОБС
высокая	Приводит к большим финансовым потерям, имеет значительное влияние на репутацию банка и может привести к остановке работы бизнес-процесса/банковского продукта	от 1,5 % до 3,0 % от величины капитала ОБС
критическая	Приводит к остановке бизнес-процесса/банковского продукта и нарушает законодательство Украины	более 3,0 % от величины капитала ОБС

Таблица 6

Оценка вероятности реализации угроз $СТП_{кол}$ нарушения ББ (влияние на конфиденциальность)

СТП нарушения ББ	Описание	$СТП_{кол}$ нарушения ББ
нереализуемая	Практически не приводит до раскрытия конфиденциальной информации	–
минимальная	Приводит к раскрытию отдельных документов, которые относятся к "банковской тайны", "коммерческой тайны", персональных данных и не приводит к финансовым потерям	–
средняя	Приводит к раскрытию отдельных документов, которые относятся к "банковской тайны", "коммерческой тайны", персональных данных и приводит к незначительным финансовым потерям	от 0,01 % до 0,5 % от величины капитала ОБС
высокая	Приводит к раскрытию документов, относящихся к "банковской тайны", "коммерческой тайны", персональных данных и приводит к значительным финансовым потерям, имеет значительное влияние на репутацию банка и может привести к остановке работы	от 0,5 % до 3,0 % от величины капитала ОБС
критическая	Приводит к остановке бизнес-процесса/банковского продукта и нарушает законодательство Украины	более 3,0 % от величины капитала ОБС

Таблица 7

Оценка вероятности реализации угроз $СТП_{кол}$ нарушения ББ (влияние на доступность)

СТП нарушения ББ	Описание	$СТП_{кол}$ нарушения ББ
нереализуемая	Практически не влияет на доступность	–
минимальная	Влияние на доступность незначительный (не более 1/10 от макс. допустимого времени простоя для этого бизнес-процесса / банковского продукта)	–
средняя	Влияние на доступность средний (не более S от максимально допустимого времени простоя для этого бизнес-процесса / банковского продукта)	от 0,01 % до 0,5 % от величины капитала ОБС
высокая	Влияние на доступность значений (до максимально допустимого времени простоя для этого бизнес-процесса / банковского продукта)	от 0,5 % до 3,0 % от величины капитала ОБС
критическая	Приводит к остановке бизнес-процесса / банковского продукта на длительное время, не превышающей максимально допустимое время простоя)	более 3,0 % от величины капитала ОБС

Примечание: Значение S ОБС выбирает самостоятельно

Таблица 8

Оценка вероятности реализации угроз $СТП_{кол}$ нарушения ББ (влияние на наблюдаемость)

СТП нарушения ББ	Описание	$СТП_{кол}$ нарушения ББ
нереализуемая	Практически не влияет	–
минимальная	Влияние практически незначительное	до 0,01 % от величины капитала ОБС
средняя	Приводит к невозможности отследить часть действий исполнителей бизнес-процесса / банковского продукта	от 0,01 % до 0,5 % от величины капитала ОБС
высокая	Приводит к невозможности отследить действия исполнителей и администраторов бизнес-процесса / банковского продукта / программно-технического комплекса	от 0,5 % до 1,5 % от величины капитала ОБС
критическая	Приводит к невозможности отследить действия исполнителей и администраторов бизнес-процесса / банковского продукта / программно-технического комплекса, может привести к остановке бизнес-процесса / банковского продукта, влияет на репутацию банка и нарушает законодательство Украины	более 1,5 % от величины капитала ОБС

Данные, на основании которых проводится оценка $СТП_{кол}$ нарушения ББ, и ее результаты документируются, для чего рекомендуется использовать примерную форму документирования данных и результатов оценки $СТП_{кол}$ нарушения ББ, приведенную в табл. 9.

Количественные оценки рисков нарушения ББ вычисляются для всех свойств ББ выделенных типов информационных активов и всех соответствующих им комбинаций объектов среды и воздействующих на них источников угроз.

Для количественной оценки целостности:

$$КОР_{ц} = \prod_{j,l=1}^{n} СВР_{кол_i}\,угроз_j ББ \times СТП_{кол_i}\,нарушения_l ББ,$$

где $КОР_{ц}$ – количественная оценка рисков целостности j-угрозы и l-нарушения; $СВР_{кол_i}\,угроз_j ББ$ – степень возможности реализации j-угрозы; $j \in \overline{1,...n}$; $СТП_{кол_i}\,нарушения_l ББ$ – степень тяжести последствий от потери свойств ББ l-нарушения j-угрозы, $l \in \overline{1,...n}$.

Для количественной оценки конфиденциальности:

$$КОР_{к} = \prod_{j,l=1}^{m} СВР_{кол_i}\,угроз_j ББ \times СТП_{кол_i}\,нарушения_l ББ,$$

где $КОР_{к}$ – количественная оценка рисков конфиденциальности j-угрозы и l-нарушения; $СВР_{кол_i}\,угроз_j ББ$ – степень возможности реализации j-угрозы; $j \in \overline{1,...m}$; $СТП_{кол_i}\,нарушения_l ББ$ – степень тяжести последствий от потери свойств ББ l-нарушения j-угрозы, $l \in \overline{1,...m}$.

Для количественной оценки доступности:

$$КОР_{д} = \prod_{j,l=1}^{q} СВР_{кол_i}\,угроз_j ББ \times СТП_{кол_i}\,нарушения_l ББ,$$

где $КОР_{д}$ – количественная оценка рисков доступности j-угрозы и l-нарушения; $СВР_{кол_i}\,угроз_j ББ$ – степень возможности реализации j-угрозы; $j \in \overline{1,...q}$; $СТП_{кол_i}\,нарушения_l ББ$ – степень тяжести последствий от потери свойств ББ l-нарушения j-угрозы, $l \in \overline{1,...q}$.

Для количественной оценки наблюдаемости:

$$КОР_{н} = \prod_{j,l=1}^{g} СВР_{кол_i}\,угроз_j ББ \times СТП_{кол_i}\,нарушения_l ББ,$$

где $КОР_{н}$ – количественная оценка рисков наблюдаемости j-угрозы и l-нарушения; $СВР_{кол_i}\,угроз_j ББ$ – степень возможности реализации j-угрозы; $j \in \overline{1,...g}$; $СТП_{кол_i}\,нарушения_l ББ$ – степень тяжести последствий от потери свойств ББ l-нарушения j-угрозы, $l \in \overline{1,...g}$.

Результаты количественной оценки рисков на-

рушения ББ документально фиксируются, для чего рекомендуется использовать примерную форму, приведенную в табл. 10.

Суммарная количественная оценка риска нарушения ББ ОБС вычислим по следующей формуле:

$$\sum \text{КОР} = \text{КОР}_{\text{ц}} + \text{КОР}_{\text{к}} + \text{КОР}_{\text{д}} + \text{КОР}_{\text{н}}$$

Размер резерва на возможные потери, связанные с инцидентами ББ, рекомендуется принимать равным суммарной количественной оценке риска нарушения ББ.

Таблица 9

Примерная форма документирования данных и результатов оценки $\text{СТП}_{\text{кол}}$ нарушения ББ при использовании методов двухфакторной аутентификации (на примере заполнения: тип информационного актива – OTP-пароль; тип объекта среды – сеансовый ключ пользователя; источник угроз – инсайдер, злоумышленник)

Тип инф. актива	Тип объекта среды	Источник угроз ББ	Свойства ББ типа инф. актива	Априорные защитные меры	Прочие данные для определения $\text{СТП}_{\text{кол}}$ нарушения ББ	Оценка $\text{СТП}_{\text{кол}}$ нарушения ББ
сеансовый ключ пользователя	ключевые данные транзакции	инсайдер	конфиденциальность	не используются	нет данных	7 млн.
			целостность	контрольное суммирование	нет данных	4 млн.
			доступность	контроль времени доступа	нет данных	3 млн.
			наблюдаемость	контроль на основе log-файлов	нет данных	0,5 млн.
		…				
		злоумышленник	конфиденциальность	не используются	нет данных	9 млн.
			целостность	контрольное суммирование	нет данных	4 млн.
			доступность	контроль времени доступа	нет данных	0,5 млн.
			наблюдаемость	контроль на основе log-файлов	нет данных	0,5 млн.

Таблица 10

Примерная форма документирования результатов оценки рисков нарушения ББ при использовании методов двухфакторной аутентификации (на примере заполнения: тип информационного актива – OTP-пароль; свойство ББ – конфиденциальность; способ реализации угрозы – “несанкционированное копирование” (НСК); тип объекта среды – сеансовый ключ пользователя; источник угроз – инсайдер, злоумышленник)

Тип инф. актива	Тип объекта среды	Источник угроз ББ	Свойства ББ типа инф. актива	Способ реализации угроз ББ	Прочие данные, $\text{СТП}_{\text{кол}}$ нарушения ББ	Оценка $\text{СВР}_{\text{кол}}$ угроз ББ	Оценка $\text{ОР}_{\text{нарушения}}$ ББ
сеансовый ключ пользователя	ключевые данные транзакции	инсайдер	конфиденциальность	НСК	7 млн.	56%	3,92 млн
		…					
	ключевые данные транзакции	злоумышленник	конфиденциальность	НСК	9 млн.	5%	0,45 млн.

Таким образом, предлагаемая методика оценки рисков нарушения ББ при использовании методов двухфакторной аутентификации позволяет оценить возможные потери, связанные с инцидентами ББ.

Выводы

1. Методы двухфакторной аутентификации на сегодняшний день рассматриваются специалистами, как механизмы усиления стойкости аутентификаторов, при обеспечении услуги аутентичности в различных сферах высоких технологий, финансового и страхового секторов рынка, крупных банковских учреждениях и предприятиях госсектора. При этом в АБС как правило используются аутентификаторы на основе OTP-паролей и различные виды токенов. Предложенный синергетический подход оценки угроз показал, что злоумышленники используют комплексный подход к реализации угроз, основанный на объединении методов социальной инженерии с традиционными методами маскарада и проникновения. Кроме этого используются и новые виды кибератак, позволяющие эффективно встраивать вредоносное ПО на мобильные средства связи, что в свою очередь приводит к снижению рентабельности методов двухфакторной аутентификации на основе SMS-сообщений и OTP-паролей в АБС.

2. Разработанная схема двухфакторной аутентификации на основе МККС Мак-Элиса и НККС Нидеррайтера позволяет устранить существенный недостаток 2FA на основе SMS-сообщений – обеспечение конфиденциальности при передаче OTP-пароля по сотовым каналам связи. Проведенные

исследования в работе подтверждают, что их применение обеспечивает быстродействие на уровне применения симметричных криптоалгоритмов с БСШ, доказуемую криптостойкость на основе теоретико-сложностной задачи декодирования случайного кода (обеспечивается $10^{30} – 10^{35}$ групповых операций), и достоверность на основе использования укороченного алгеброгеометрического кода (обеспечивается $P_{ош}$ $10^{-9} – 10^{-12}$). Существенным недостатком применения криптосистемы Мак-Элиса являются большие объемы ключевых данных (для обеспечения требуемой криптостойкости необходимо построение системы в поле $GF(2^{10} – 2^{13})$. Для уменьшения объемов ключевых данных (открытого ключа) в работе предлагается использовать укороченные коды, что позволяет уменьшить поле $GF(2^6 – 2^7)$, сохранив при этом уровень криптостойкости, за счет внесения энтропии расположения символов вектора инициализации.

3. Предлагаемая методика оценки рисков нарушения банковской безопасности при использовании методов двухфакторной аутентификации позволяет количественно (в денежной форме) оценить возможные потери, связанные с инцидентами банковской безопасности.

Список литературы

1. • Решение по многофакторной аутентификации 2FA One [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/1cloud/blog/277901.

2. Двухфакторная аутентификация [Электронный ресурс]. – Режим доступа: http://www.smspasscode.ru/product/two-factor-authentication.

3. Клювак О.В. Аналіз методів аутентифікації за допомогою банківських карток в інтернет-платіжних системах / О.В. Клювак, С.С. Королюк, А.А. Засядько // Системи обробки інформації. – Х.: ХУПС, 2012. – Вип. 4(102). – С. 122 – 127.

4. Евсеев С.П. Алгоритм мониторингу метода двухфакторной аутентификации на основе системы Passwindow // С.П. Евсеев, В.Г. Абдуллаев / Восточно-европейский журнал передовых технологий. – Х., 2015. – Вып. 2/2(74). – С. 9 – 15.

5. Обойти двухфакторную аутентификацию можно [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/news/453062.php.

6. Евсеев С.П. Синергетический подход к оценке безопасности банковских систем // Системи обробки інформації. – Х.: ХУПС, 2016. – Вип. 4 (141). – С. 90 – 103.

7. Двухфакторная аутентификация или 2FA [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/1cloud/blog/277901.

8. Евсеев С.П. Исследование методов двухфакторной аутентификации / С.П. Евсеев, О.Г. Король // Системи обробки інформації. – 2014. – Вип. 2(118). – С. 81– 87.

9. Пять способов двухфакторной аутентификации [Электронный ресурс]. – Режим доступа: https://lifehacker.ru/2016/02/15/two-factor-authentication/

10. RSA SECURID® Аутентификация по запросу [Электронный ресурс]. – Режим доступа: http://security.demos.ru/auth_access/mfa/ondemand.php

11. Семь методов двухфакторной аутентификации [Электронный ресурс]. – Режим доступа: http://www.infosecurityrussia.ru/news/29947

12. Блейхут Р. Теория и практика кодов, контролирующих ошибки [Текст]. – М.: Мир, 1986. – 576 с.

13. Кларк Дж.-мл. Кодирование с исправлением ошибок в системах цифровой связи [Текст]. – М. : Радио и связь, 1987. – 392 с.

14. Мак-Вильямс Ф.Дж. Теория кодов, исправляющих ошибки [Текст] / Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн. – М.: Связь, 1979. – 744 с.

15. Евсеев С.П. Разработка модифицированной несимметричной крипто-кодовой системы Мак-Элиса на укороченных эллиптических кодах / С.П. Евсеев, Х.Н. Рзаев, О.Г. Король // Восточно-европейский журнал передовых технологий. – Харьков. – 2016. – Вып. 4/9(82). – С. 4 – 12.

16. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Текст]: лист департаменту інформатизації Нац. банку України банкам України від 03.03.2011 р. № 24-112/365. – К.: Національний банк України, 2011.

17. РС БР ИББС-2.2-2009. Методика оценки рисков нарушения информационной безопасности. [Електронний ресурс]. – 2009. – Режим доступу до ресурса: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf

Надійшла до редколегії 10.06.2016

Рецензент: д-р техн. наук, проф. В.О. Хорошко, Національний авіаційний університет, Київ.

ВДОСКОНАЛЕННЯ МЕТОДУ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ НА ОСНОВІ ВИКОРИСТАННЯ МОДИФІКОВАНИХ КРИПТО-КОДОВИХ СХЕМ

С.П. Євсеєв, В.Г. Абдуллаєв, Ж.Ф. Агазаде, В.С. Аббасова

Розглянуто класифікацію методів двофакторної автентифікації, основні переваги та недоліки методів. Пропонується схема двофакторної автентифікації на основі SMS-повідомлень з використанням модифікованої крипто-кодової схеми Мак-Еліса і Нідеррайтера, методика оцінки ризиків використання методів двофакторної автентифікації, розглянуті практичні алгоритми побудови несиметричних крипто-кодових систем.

Ключові слова: *двофакторна автентифікація, модифікована крипто-кодова схема Мак-Еліса і Нідеррайтера.*

IMPROVING THE METHOD OF TWO-FACTOR AUTHENTICATION BASED ON THE USE OF MODIFIED CRYPTO-CODE SCHEMES

S.P. Yevseiev, V.H. Abdullayev, J.F. Agazadeh, V.S. Abbasova

Considered classification of two-factor authentication methods, the main advantages and disadvantages of the methods. Proposed two-factor authentication scheme on the basis of SMS-messages using McEliece and Niederreiter modified crypto-code scheme, methodology for risk assessment of the use of two-factor authentication methods considered practical algorithms for constructing asymmetrical crypto-code systems.

Keywords: *two-factor authentication, McEliece and Niederreiter modified crypto-code scheme.*