Викладається сутність і обґрунтовується необхідність застосування механізмів багатофакторної автентифікації. Пропонуються моделі оцінки захищеності від несанкціонованого доступу для випадків, коли в якості факторів автентифікації використовуються асиметричні криптографічні перетворення, системи паролювання, біометричні ознаки. Розглядаються й аналізуються за критеріями стійкості і складності асиметричні криптографічні перетворення, робляться рекомендації щодо їх застосування на практиці

Ключові слова: несанкціонований доступ, багатофакторна автентифікація, механізм паролювання, біометричні ознаки, особистий ключ

Излагается сущность и обосновывается необходимость применения механизмов многофакторной аутентификации. Предлагаются модели оценки защищенности от несанкционированного доступа для случаев, когда в качестве факторов аутентификации используются асимметричные криптографические преобразования, системы паролирования, биометрические признаки. Рассматриваются и анализируются по критериям стойкости и сложности асимметрические криптографические преобразования, делаются рекомендации по их применению на практике

Ключевые слова: несанкционированный доступ, многофакторная аутентификация, механизм паролирования, биометрические признаки, личный ключ

УДК 004.056.53

МОДЕЛИ И МЕТОДЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ МЕХАНИЗМОВ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Ю. И. Горбенко
Кандидат технических наук,
старший научный сотрудник*
E-mail: GorbenkoU@iit.com.ua
И. В. Олешко
Аспирант*
E-mail: InnaG88@gmail.com
*Кафедра безопасности
информационных технологий
Харьковский национальный университет
радиоэлектроники
пр. Ленина, 16, г. Харьков, Украина, 61166

1. Введение

Сейчас в технологически развитых государствах особое внимание уделяется проблемам кибербезопасности, разработаны и реализовываются доктрины информационной безопасности [1]. Основным содержанием доктрин является противодействие угрозам безопасности, прежде всего – защите от несанкционированного доступа (НСД) к информации и информационным ресурсам (в основном за счет использования иностранных информационных технологий, механизмов, протоколов и техники), а также компьютерной преступности и компьютерного терроризма. Их реализация составляет угрозу стабильному функционированию информационно–телекоммуникационных систем (ИТС), а в некоторых случаях приводит или может привести к недопустимым потерям. Убедительным подтверждением этому являются приведенные в ряде источников факты [2], например систематических и многочисленных взломов сайтов, НСД с последующим искажением информационных ресурсов и баз данных различной степени критичности и т.п. Указанные выше угрозы предопределяют необходимость теоретической и практической разработки и применения механизмов и средств противодействия угрозам кибербезопасности [1]. На первом шаге реализации механизмов защиты стоят системы и средства защиты от НСД.

2. Постановка проблемы

На наш взгляд, одним из основных направлений совершенствования механизмов и средств защиты от НСД является теория и практика аутентификации. Необходимо также подчеркнуть, что на решение этой проблемы в будущем цифровом мире Европейского Союза (ЕС) предполагается обязательное предоставление пользователям таких услуг как электронная идентификация, электронная аутентификация и электронная аутентификация сайтов и информационных ресурсов [3]. Дело в том, что в настоящее время широкое распространение получили в основном системы и средства аутентификации, которые базируются на применении механизмов паролирования. Исследования показывают, что решение проблем обеспечения защиты от НСД может быть обеспечено на основе применения механизмов многофакторной аутентификации [4 – 7]. Целью этой статьи является разработка основных теоретических и практических положений в части математической модели оценки защищенности от НСД, а также обосновании выбора факторов аутентификации, методов их анализа и оценки.

Исследования показали [4 – 11], что ныне единых подходов к построению и оценке защищенности механизмов многофакторной аутентификации от НСД в известной литературе не выявлено. Поэтому, на наш взгляд, проблемными и такими, которые требуют раз-

решения, являются следующие научные задачи в области криптологии:

1. Обоснование и выбор критериев и показателей оценки защищенности ИТС и электронных средств от НСД.

2. Теоретическое обоснование и разработка математических моделей оценки механизмов многофакторной аутентификации от НСД.

3. Разработка методов и методических положений обоснования и выбора факторов аутентификации, а также оценки и выбора предпочтительных факторов для механизмов многофакторной аутентификации.

4. Оценка и сравнительный анализ одно, двух и трех факторных механизмов аутентификации по критерию защищенности от НСД, а также распространение на общий случай многофакторной аутентификации.

5. Разработка предложений и рекомендаций по применению механизмов многофакторной аутентификации.

В настоящем разделе излагаются основные положения и подходы к решению задач, которые приведенные выше. Необходимо также заметить, что речь идет об основных положениях.

В дальнейшем под механизмами многофакторной аутентификации будем понимать механизмы установления подлинности объектов и/или субъектов, в которых используется, по крайней мере, два независимых фактора аутентификации.

При этом практически могут использоваться следующие факторы различной природы [12]:

• знания - то есть информация, которую знает субъект, например: пароль, пин-код, личный ключ;

• знание - сущность, которой располагает субъект, например: электронная или магнитных карта, флеш-память, электронный ключ и т.п.;

• свойство, которым обладает субъект, например биометрические признаки: лицо, отпечатки пальцев, радужная оболочка глаза, капиллярные узоры, ДНК и т.д.

3. Модели оценки защищенности механизмов многофакторной аутентификации от НСД

При построении схем многофакторной аутентификации могут использоваться механизмы с последовательным, параллельным или комбинированным применением факторов. Под последовательным применением факторов будем понимать такое их использование, при котором ошибка хотя бы по одному из них, то есть получение НСД, приводит к отказу в доступе. То есть, последовательная структура многофакторной аутентификации работоспособна, если все ее факторы вместе обеспечивают с определенной вероятностью отказ в несанкционированном доступе. Последовательный механизм факторной аутентификации можно использовать при построении схем многофакторной аутентификации. При таких условиях для противодействия НСД необходимо, чтобы хотя бы один фактор не был пройденным успешно. То есть, последовательная схема аутентификации работоспособна, если все ее элементы работоспособны. Под параллельным использованием факторов аутентификации будем понимать такое их одновременное применение, при котором НСД происходит тогда, когда хотя бы по одному из них получен НСД. В тоже время, параллельные схемы аутентификации могут, а по сущности должны, когда их несколько, применяться последовательно. В этом случае необходимо говорить о комбинированном механизме аутентификации.

Рассмотрим сначала комбинированные схемы многофакторной аутентификации с параллельно-последовательным соединением элементов. В этом случае возможно использование нескольких факторов – например паролей, личных ключей и биометрических признаков [5 – 7]. Структурные схемы реализации механизмов трех- и двухфакторной аутентификации приведены на рис. 1, 2.

Рассмотрим модель оценки для случая трехфакторной аутентификации, понимая, что механизмы двух и одно факторной аутентификации являются частными случаями, а от трехфакторной аутентификации легко перейти к многофакторной.

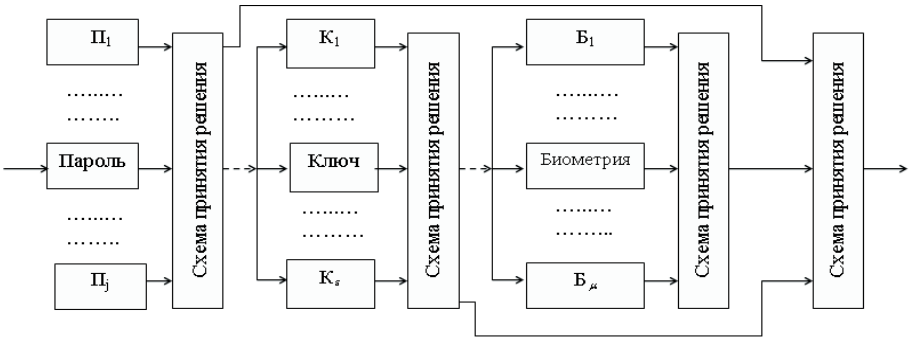

Рис. 1. Комбинированный механизм трехфакторной аутентификации «пароль — ключ — биометрия»

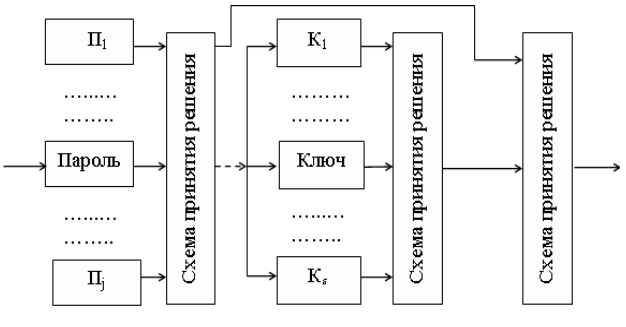

Рис. 2. Комбинированный механизм двухфакторной аутентификации «пароль — ключ»

Подобным образом можно представить и другие модели механизмов двухфакторной аутентификации - «ключ - биометрия» и «пароль - биометрия».

Утверждение 1. Вероятность НСД для механизма аутентификации, представленного на рис. 1, определяется по формуле:

$$P_{НСД} = \left(1 - \prod_{i=1}^{j} P_i^{n}\right)\left(1 - \prod_{i=1}^{\varepsilon} P^{k}{}_i\right)\left(1 - \prod_{i=1}^{\mu} P^{б}{}_i\right), \quad (1)$$

где $P^{n}{}_i$ – вероятность правильной работы механизма паролирования;

$P^{k}{}_i$ – вероятность правильного применения механизма личного ключа;

$P^{б}{}_i$ – вероятность правильного применения механизма биометрического признака.

Доказательство соотношения (1) сводится к следующему. Для первой схемы значение вероятностей $P^{п}{}_{нсд}$ и $P^{п}{}_{защ}$, т.е. в случае применения пароля, имеем:

$$P_{нсд} + P_{защ} = 1. \quad (2)$$

Далее

$$P_{нсд} = 1 - P_{защ}. \quad (3)$$

Теперь определим вероятность правильной работы механизма аутентификации $P^{п}{}_{защ}$. Это произойдет в том случае, если ни по одному из каналов введения пароля не будет НСД, тогда согласно (3):

$$P^{n}{}_{нсд} = 1 - P^{n}{}_{защ} = 1 - P_1^{n} P_2^{n} \ldots\ldots P_j^{n} = 1 - \prod_{i=1}^{j} P^{n}{}_i, \quad (4)$$

где $P^{п}{}_1$ $P^{п}{}_2$ ..... $P^{п}{}_i$ – соответственно вероятности отказа в НСД при разрешении применения паролей всех J пользователей.

По аналогии, для случая оценки вероятности НСД за счет применения пользователями личных ключей имеем, что

$$P^{k}{}_{нсд} = 1 - P^{k}{}_{защ} = 1 - P_1^{k} P_2^{k} \ldots P_{\varepsilon}^{k} = 1 - \prod_{i=1}^{\varepsilon} P^{k}{}_i. \quad (5)$$

Для случая оценки вероятности НСД за счет применения биометрических признаков имеем, что

$$P^{б}{}_{нсд} = 1 - P^{б}{}_{защ} = 1 - P_1^{б} P_2^{б} \ldots P_{\mu}^{б} = 1 - \prod_{i=1}^{\mu} P_i^{б}. \quad (6)$$

Так как события получения НСД по всем трем факторам независимы, то общая вероятность НСД определяется в виде (1), а вероятность защищенности

$$P_{нсд} = \prod_{i=1}^{j} P_i^{n} \prod_{i=1}^{\varepsilon} P^{k}{}_i \prod_{i=1}^{\mu} P_i^{в}. \quad (7)$$

Такое же доказательство справедливо и для произвольной многомерности применения факторов аутентификации. Практическое значение также имеют частные случаи, когда применяется два или один из трех факторов аутентификации. В табл. 1 приведены частные случаи моделей оценки для трех вариантов двухфакторных механизмов.

В первой строке приведены значения, которые соответствуют модели, представленной на рис. 2. Используя приведенные соотношения, можно оценить $P_{нсд}$ ($P_{защ}$) механизмов комбинированной двухфакторной аутентификации.

На рис. 3 представлена последовательно – параллельная модель механизма трехфакторной аутентификации типа «пароль - биометрия - ключ».

В частном случае она может быть сведена к последовательному механизму, который представлен на рис. 4.

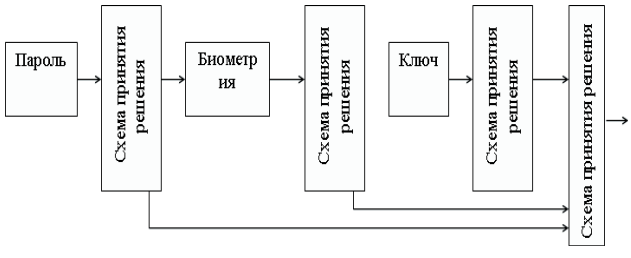

Рис. 3. Последовательно – параллельный механизм трехфакторной аутентификации «пароль – биометрия – ключ»

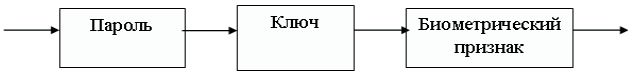

Рис. 4. Последовательное соединение трехфакторного механизма защиты от НСД

Вероятность НСД в последовательной структуре нужно определять по теореме умножения вероятностей.

В этом случае вероятность произведения нескольких независимых событий равна произведению вероятностей этих событий.

Для этого случая имеем, что

$$P_{нсд} = P^{нсд}{}_{п} \cdot P^{нсд}{}_{к} \cdot P^{нсд}{}_{б} = (1 - P_{п})(1 - P_{к})(1 - P_{б}), \quad (8)$$

где $P_{п}$ – вероятность правильного применения пароля;

$P_{к}$ - вероятность правильного применения ключа;

$P_{б}$ - вероятность правильного применения биометрических данных;

$P^{нсд}{}_{п}$ – вероятность подделки пароля;

$P^{нсд}{}_{к}$ – вероятность подделки ключа;

$P^{нсд}{}_{б}$ – вероятность подделки биометрических данных.

Таблица 1

Соотношения для оценки $P_{нсд}$ ($P_{защ}$) механизмов комбинированной двухфакторной аутентификации

Механизм пароль/ключ	$P_{нсд} = \left(1 - \prod_{i=1}^{j} P_i^{n}\right)\left(1 - \prod_{\partial=1}^{\varepsilon} P^{к}{}_{\partial}\right)$	$P_{защ} = \prod_{i=1}^{j} P_i^{n} \cdot \prod_{j=1}^{\varepsilon} P^{к}{}_j$
Механизм пароль/биометрия	$P_{нсд} = \left(1 - \prod_{i=1}^{j} P_i^{n}\right)\left(1 - \prod_{l=1}^{\mu} P^{б}{}_l\right)$	$P_{защ} = \prod_{i=1}^{j} P_i^{n} \cdot \prod_{l=1}^{\mu} P^{б}{}_l$
Механизм ключ/биометрия	$P_{нсд} = \left(1 - \prod_{\partial=1}^{\varepsilon} P^{к}{}_{\partial}\right)\left(1 - \prod_{l=1}^{\mu} P^{б}{}_l\right)$	$P_{защ} = \prod_{j=1}^{\varepsilon} P^{к}{}_j \cdot \prod_{l=1}^{\mu} P^{б}{}_l$

Далее, вероятность безотказной (правильной) работы последовательной структуры для случая, изображенного на рис. 4, определяется по формуле:

$$P_{защ} = 1 - P_{нсд} = 1 - (1 - P_п)(1 - P_к)(1 - P_б). \quad (9)$$

Также практическое значение имеют частные случаи, когда применяется один или два фактора аутентификации.

В табл. 2 приведены частные случаи моделей оценки для трех вариантов двухфакторных механизмов аутентификации. Используя приведенные соотношения, можно оценить $P_{защ}$ и $P_{нсд}$ механизмов последовательной двухфакторной аутентификации.

В табл. 1 и 2 приведены аналитические соотношения, которые можно использовать при оценке защищенности от НСД в случае параллельного или последовательного применения одного фактора аутентификации.

Таблица 2

Соотношения для оценки $P_{нсд}$ ($P_{защ}$) механизмов последовательной двухфакторной аутентификации

Механизм пароль/ключ	$P_{нсд} = (1 - P_п)(1 - P_к)$	$P_{защ} = 1 - (1 - P_п)(1 - P_к)$
Механизм пароль/биометрия	$P_{нсд} = (1 - P_п)(1 - P_б)$	$P_{защ} = 1 - (1 - P_п)(1 - P_б)$
Механизм ключ/биометрия	$P_{нсд} = (1 - P_к)(1 - P_б)$	$P_{защ} = 1 - (1 - P_к)(1 - P_б)$

4. Методы оценки защищенности от НСД при использовании асимметрических криптопреобразований

В общей постановке сущность методов оценки защищенности от НСД при использовании асимметричных криптографических преобразований формулируется следующим образом. В случае применения для защиты от НСД в качестве фактора аутентификации личного ключа, необходимо обосновать и выбрать методы криптографических преобразований, для каждого из методов определить и произвести классификацию атак со стороны существующих или потенциальных криптоаналитиков (нарушителей), выбрать критерии и показатели, которые позволили бы их сравнить и выбрать такие атаки, которые могут быть реализованы и обеспечивали бы достижение максимальных значений вероятностей НСД для нарушителя.

Также необходимо дать им оценку и сделать сравнительный анализ относительно сложности компрометации личного ключа, и в целом асимметричной пары для каждого из асимметричных криптографических преобразований, сформулировать предложения и рекомендации, в том числе для применения в механизмах многофакторной аутентификации.

Предварительный анализ позволил выбрать для исследований ряд асимметричных криптографических преобразований. В табл. 3 приведены обобщенные данные о выбранных для исследований асимметричных криптографических преобразованиях типа электронной цифровой подписи, а также асимметричные ключевые пары [4 – 7, 13]. Эти преобразования нашли или находят применение, в большинстве апробированы и стандартизированы.

Указанное является важным с точки зрения применения и оперативного внедрения результатов исследований.

Данные в табл. 3 можно рассматривать и как некую классификацию асимметрических криптопреобразований, а также как результат сравнения их устойчивости против атаки «полное раскрытие». На основе [6, 7] и данных табл. 3 в качестве факторов аутентификации будем использовать асимметричные пары ключей - преобразования в кольцах (алгоритм RSA), в поле Галуа (DSA), в группе точек эллиптических кривых и спаривания точек эллиптических кривых. Вероятность НСД к ключам может быть определена на основе атаки полный перебор, а также на основе решения задач полного раскрытия, например, для RSA - это факторизация модуля преобразований. Выбор атаки будем делать, руководствуясь принципом минимальной сложности для нарушителя (криптоаналитика), осуществляющего НСД.

Таблица 3

Параметры и ключи асимметрических криптопреобразований для ЕЦП [13 - 18]

Параметры и ключи/стандарт ЕЦП	Асиметричная пара (ключи)	Личный ключ ЦП	Открытый ключ ЕЦП	Общие параметры ЕЦП	Сложность криптоанализа
Преобразование RSA	(E_i, D_i)	E_i	D_i	$N = PQ$	субэкспоненциальная
Преобразование DSA (ГОСТ Р 34.10-94)	(x_i, Y_i)	X_i	$Y_i = g^{x}_i (\mathrm{mod}\ P)$	P, q, g	субэкспоненциальная
ДСТУ 4145- 2002 (ISO/ IEC14888-3, ISO/IEC 9796-3)	(d_i, Q_i)	d_i	$Q_i = d_i G (\mathrm{mod} q)$	a, b, G, n, f(x)(P), h	экспоненциальная
Спаривание точек эллиптических кривых	$(d_i D, Q_i D)$	$D_i = s\ Q_i D$	$Q_i D = H_1(ID)$	G_1, G_2, e, H_1, P, H_2, H_3, F^{2m}, P_p	Между экспоненциальной и субэкспоненциальной

Преобразование RSA. Анализ показал, что сущность задач криптоанализа для криптографических преобразований RSA методом полного раскрытия сводится к определению личного (конфиденциального) ключа, а по сути факторизации модуля. В табл. 4 приведены формулы для расчета сложности факторизации соответствующих методов. Наиболее простым (быстрым) алгоритмом является решето числового поля [7].

Таблица 4

Сложность факторизации модуля RSA преобразования

Название метода	Сложность метода
Грубая сила	$O(N^{1/2})$
ρ-Полларда метод	$O(N^{1/4})$
Метод квадратичных форм Шенкса	$O(N^{1/4})$
Метод Диксона	$L_N(1/2,\ 2\sqrt{2}\ )$
Метод непрерывных дробей	$L_N(1/2,\ \sqrt{2}\ )$
Метод квадратичного решета	$L_N(1/2,1)$;
Метод эллиптических кривых	$L_p(1/2,\ \sqrt{2}\ )$
Метод решета числового поля	$L_N(1/3,(64/9)^{1/3})$
Метод специального решета числового поля	$L_N(1/3,(32/9)^{1/3})$
Полиномиальный метод Чалмерса	$\ln^m N$, $4<m<5$

Преобразование в конечном поле. В табл. 5 приведены аналитические выражения, которые могут быть применены для оценки сложности соответствующих методов дискретного логарифмирования [6].

Таблица 5

Сложность дискретного логарифмирования в конечном поле (Галуа)

Название метода	Сложность метода
ρ-Полларда метод	$O(P^{1/2})$
Метод Полига-Геллмана при $P-1=\prod_{i=1}^{s} q_i^{\alpha_i}$	$O(\sum_{i=1}^{s}\alpha_i(\log P+q_i))$
Метод Адлемана (δ , v – константы), $0\le v<1$	$O(\exp(\delta(\ln(P)\ln(\ln(P)))^v))$
Метод Купершмидта (δ =1,56, v=1/2)	$O(\exp(\delta(\ln(P)\ln(\ln(P)))^v))$
Метод решета числового поля [19]	$O(\exp(3^{3/2}(\ln(P)\ln(\ln(P)))^{1/3}))$
Метод решета числового поля [20]	$\exp((64/9)^{1/3}(\ln q)^{1/3}(\ln\ln q)^{2/3})$

Их анализ подтверждает, что методы ρ - Полларда и Полига - Геллмана имеют экспоненциальную сложность, а методы Адлемана, Купершмидта и решета числового поля имеют субэкспоненциальную сложность дискретного логарифмирования. Исходя из таблицы и данных, можно сделать вывод о том, что наиболее простым (быстрым) методом дискретного логарифмирования является решето числового поля.

Дискретное логарифмирование в группе точек эллиптических кривых. Осуществление атаки «полное раскрытие» в группе точек эллиптических кривых непосредственно связано с решением задачи дискретного логарифмирования в группе точек эллиптической кривой. Основной задачей при этом является нахождение личного ключа d_i на основе обращения сравнения вида (нахождения d_i):

$$Q_i = d_i \cdot G(\mathrm{mod}\, q). \qquad (10)$$

Результатом обращения является компрометация личного ключа d_i, который может быть использовано злоумышленником для осуществления НСД. Сложность решения этого сравнения намного выше, чем в кольце (RSA) и конечным поле (DSA) и носит экспоненциальный характер.

Наиболее быстрым (менее сложным) алгоритмом атаки типа «полное раскрытие» случайных «неслабых» кривых над полями, и, как показано в [8], в настоящее время является параллельный метод ρ - Полларда. Его сложность оценивается как зависимость вида:

$$I^2 - I + 2n\ln(1-P_k) = 0, \qquad (11)$$

где I – сложность атаки «полного раскрытия», n – порядок базовой точки, P_k – вероятность решения задачи.

Далее рассмотрим оценки стойкости ЭЦП в группе точек эллиптических кривых к атаке экзистенциальная подделка, селективная подделка, атаке на связанных ключах, атаке на программную реализацию и атаке специального вида [6]. В целом необходимо отметить, что практически от всех атак можно защититься, исключая атаку грубая сила и «полное раскрытие». Поэтому оценку защищенности от НСД при использовании в качестве фактора аутентификации личного ключа будем осуществлять на основе оценки сложности осуществления атаки «полное раскрытие».

Методы криптоанализа в фактор-кольцах [6]. Сейчас криптопреобразования в кольцах срезанных полиномов находят значительное распространение и реализуются в виде криптосистемы NTRU. Указанное можно объяснить двумя их свойствами - экспоненциальным характером решения задач «полного раскрытия» и существенно повышенным быстродействием по сравнению с другими криптопреобразованиями, которые рассмотрены выше в этом разделе. Известные атаки можно разделить на два основных типа - грубой силы и аналитические, которые, в свою очередь, основываются на методах возведения в решетках. Оба метода могут быть использованы при криптоанализе, при этом основной задачей криптоанализа является нахождение личного ключа.

В табл. 6 приведены обобщенные данные относительно сложности криптоанализа в фактор - кольцах.

При использовании соответствующих параметров можно оценить вероятность НСД для случая использования в качестве фактора аутентификации личного ключа. Соответствующие соотношения приведены в табл. 6 и могут быть взяты из [6]. Вероятности НСД относительно личного ключа для всех названных асимметричных систем будут малы. Их значения можно изменять в зависимости от выбранных параметров и вида асимметричного преобразования.

Таблица 6

Сложность криптоанализа в фактор – кольцах

Название метода	Сложность метода
Задачи SVP и CVP анализа	$2^{O(n(\log\log n)\wedge 2/\log n)}$
Алгоритм BKZ-LLL нахождения ненулевого вектора v	$O(n^2(\beta^{\beta/2+o(\beta)} + n^2))$.
Нахождение самого короткого вектора (алгоритм) BKZ-LLL	$O(n^2\beta^{\beta/2})$ або $O(n^3(k/6)^{k/4})$
Задачи SVP та CVP(время работы)	$2O(n \log n)$
Лобовая атака на решетку	$T = 2^{(0.4N-3,5)}$.
Атака грубая сила	$T = C_N^{d_f} C_{N-d_f}^{d_f-1}$
Атака встреча посередине	$I = C_{N/2}^{d_f/2}$
Комбинаторная атака на ЭЦП	$\omega(N,d) = \log_2\left(\frac{N}{\frac{d+1}{\sqrt{N}}}\right)$.
Атака на основе угадывания позиций нулей	$\omega_{lk}(N,d,A,B,A_{ZF},B_{ZF}) = \log_2(T_{normal}) - \max_{0\le r\le 2N-2d-1}\{\log_2(\delta)\}$
Атака подделывания подписи	$P(\text{combinatorial forgery}) \approx \sqrt{\frac{\pi^{\frac{N-1}{2}}}{q^{N-1}(\frac{N-1}{2})!}\left(\frac{N}{\beta}\right)^{N-1}} < 2^{-k}$

Анализ показывает, что используя соответствующие параметры NTRU НШ можно оценить вероятность НСД для случая использования в качестве фактора аутентификации личного ключа ЕЦП. Соответствующие соотношения приведены в табл. 6 и могут быть взяты из [18].

Таким образом, предложены методы оценки защищенности механизмов аутентификации от НСД, которые основаны на использовании асимметричных криптопреобразований. Основой такой защиты является использование личных ключей асимметричных криптопреобразований. Вероятности НСД относительно компрометации личного ключа для всех названных асимметричных систем можно изменять, в зависимости от выбранных параметров и вида преобразования, а также от возможностей криптоаналитика.

5. Выводы

В ходе выполнения работы было выявлено следующее:

1. В качестве основных факторов аутентификации можно использовать: свойство, которым обладает субъект; знание – то есть информацию, которую знает субъект; владение - сущность, которой располагает субъект. Например, электронный ключ и т.п.

2. При построении механизмов многофакторной аутентификации могут использоваться отдельные указанные выше механизмы и объединятся последовательным, параллельным или комбинированным соединением элементов, реализующих факторы аутентификации.

3. Комбинированные схемы многофакторной аутентификации строятся на основе параллельно-последовательного соединения элементов (факторов), когда, например, возможно использование нескольких факторов: паролей, биометрических признаков, личных ключей и т.п.

4. В статье предложены математические модели механизмов многофакторной аутентификации, при использовании которых можно оценить вероятности осуществления НСД на основе комбинированных и последовательных механизмов аутентификации. Разработанные математические модели могут быть распространены на произвольный размер пространства аутентификации и носят общий характер.

5. В процессе построения системы защиты от НСД сначала предпочтительно определить перечень факторов, которые можно применить для осуществления многофакторной аутентификации. Затем для каждого из факторов определить полный перечень атак с существующих или потенциальных криптоаналитиков и дать им оценки. После этого можно принимать решение относительно выбранных факторов.

6. При использовании в качестве фактора аутентификации криптографических преобразований необходимо конкретизировать метод криптографического преобразования, который будет применяться; для каждого из методов определить и произвести классификацию атак, обосновать и выбрать методы криптографического анализа, выбрать критерии и показатели, которые позволили бы их сравнить и выбрать наиболее уязвимые атаки, которые могут быть осуществлены в целях НСД; получить оценки и сформулировать предложения и рекомендации для защиты от НСД, когда фактором является личный ключ и носитель, на котором он хранится.

7. При применении в качестве фактора аутентификации биометрических признаков, необходимо обосновать и выбрать конкретный биометрический признак, критерии и показатели, которые позволили бы дать ему оценку, при условии достижения нарушителем

минимальных значений вероятностей НСД, сформулировать предложения и рекомендации относительно применения и защищенности от НСД соответствующего биометрического признака.

8. Результаты оценки вероятности НСД относительно личного ключа для всех асимметричных систем при осуществлении атаки «полное раскрытие» в зависимости от размеров системных параметров и ключей могут быть сделаны бесконечно малыми. Но могут существовать другие виды атак, перечень которых должен обосновываться соответствующим образом. Например, заказчик может требовать, чтобы система была устойчивой относительно атак типа «грабительский анализ». При таких условиях обеспечение необходимого уровня защиты от НСД может переводиться на аппаратные или аппаратно-программные носители ключей или другие факторы. При таких обстоятельствах два или три фактора все же могут обеспечить необходимый уровень защищенности от НСД.

9. При трехфакторной аутентификации значение вероятности НСД зависит от вероятностей НСД для каждого из факторов. Но, как показывает анализ, для получения оценки нужно обосновать и конкретизировать метод осуществления атаки для каждого из факторов и определить для каждого из методов возможность реализации, возможные погрешности и т.п.

10. Полученные научные и практические результаты подтвердили возможность реализовать метод многофакторной аутентификации. В зависимости от требований и модели угроз для защиты от НСД может быть использована как двухфакторная, так и трехфакторная аутентификация.

11. Безусловно, что в дальнейшем при практическом построении механизмов многофакторной аутентификации необходимо провести ряд исследований и получить оценки относительно их защищенности от НСД для конкретных моделей угроз и применяемых ключей и параметров.

Литература

1. ISO/IEC 27032:2012(E). Information technology – Security techniques – Guidelines for cybersecurity [Text]. – 2012 – 07 – 01. – G.: ISO copyright office, 2012. – 50 p.
2. Perlroth, N. N.S.A. Able to Foil Basic Safeguards of Privacy on Web / N. Perlroth, J. Larson, S. Shane [Electronic resource] // The New York Times, September 5, 2013: Newspaper. – Mode of access: http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html.
3. Proposal for a regulation of the european parliament and of the council on electronic identification and trust services for electronic transactions in the internal market [Text]: COM(2012) 11 final. - European Commission 04.06.2012. – Brussels: Europian Commission, 2012. – 119 p.
4. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. [Текст] / Б. Шнайер. - 2-е изд. - М.: ТРИУМФ, 2002. - 816 с.
5. Столлингс, В. Криптография и защита сетей. Принципы и практика. [Текст] / В. Столлингс. - 2-е изд. - М.: Вильямс, 2001. - 672 с.
6. Горбенко, І. Д. Прикладна криптологія. [Текст]: монографія / І. Д. Горбенко, Ю. І. Горбенко; ХНУРЕ. – Х.: Форт, 2012. - 868 с.
7. Горбенко, Ю. І. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика [Текст] / Ю. І. Горбенко, І. Д. Горбенко. – Х.: Форт, 2010. – 593 с.
8. Симонс, Г. Д. Обзор методов аутентификации информации [Текст] / Г. Д. Симонс. – М: ТИИЭР, 1988. – Т.76, №5. – С. 105-125.
9. ISO/IEC 9798-1 Information technology – Security techniques – Entity authentication – Part1: General [Text]. – 2010 – 07 – 01. – G.: ISO copyright office, 2010. – 11 p.
10. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння [Текст]. – введ. 2002 - 28 - 12. - К.: Госпотребстандарт, 2002. – 38 с.
11. ДСТУ ISO/IEC 9798-3-2002 Інформаційні технології. Методи захисту. Автентифікація суб'єктів. Частина 3. Механізми з використанням методу цифрового підпису [Текст]. – введ. 2005 – 09 - 2005. - К.: Госпотребстандарт, 2005. – 17 с.
12. Горбенко, И. Д. Метод оценки относительной энтропии и сравнительный анализ источников биометрической информации [Текст] / И. Д. Горбенко, И. В. Олешко // Прикладная радиоэлектроника: Научно-техн. журнал. - 2012. - Том 11, № 2. - С. 255-261
13. ISO/IEC 11770-3:2008 Information technology. Security techniques. Key management mechanisms using asymmetric techniques [Text]. – 2008 – 07 – 31. – G.: BSI, 2008. – 94 p.
14. ISO/IEC 9797-1 Information technology – Security techniques – Message Authentication Codes (MACs). Mechanisms using a block cipher [Text]. – 2011 – 03 – 31. - G.: BSI, 2011. – 52 p.
15. ISO/IEC 9797-2 Information technology. Security techniques. Message Authentication Codes (MACs). Mechanisms using a dedicated hashfunction [Text]. – 2011 – 05 – 31. – G.: BSI, 2011. – 50 p.
16. ISO/IEC 14888-3:2006 Information technology. Security techniques. Digital signatures with appendix. Discrete logarithm based mechanisms [Text]. – 2006 – 12 - 29. – G.: BSI, 2006. – 114 p.
17. ISO/IEC 9796-3:2006 Information technology. Security techniques. Digital signature schemes giving message recovery. Discrete logarithm based mechanisms [Text]. – 2006 – 10 – 31. - G.: BSI, 2006. – 80 p.
18. ANSI X9. 98 – 2010. Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry [Text]. – 2010 – 10 – 15. – NY: ASME, 2010. – 297 p.
19. Abe, M. A signature scheme with message recovery as secure as discrete logarithm [Text]: Advances in Cryptology - Asiacrypt 1999, Lecture notes in computer science (1999) / M. Abe, T. Okamoto. – B.: Springer-Verlag, 1999. – pp. 378-389.
20. Maier, W. Fast correlation attacks on certain stream ciphers [Text] / W. Maier, O. Staffelbach // Journal of Cryptology. – 1989. - Volume 1, Issue 3. - pp. 159-176.