Индекс 79187

ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

3

(130)

Подписывайтесь,

читайте,

пишите в наш журнал

Москва 2020

Все новейшие достижения и современные разработки предприятий оборонного комплекса — в научно-технических журналах ФГУП «НТЦ оборонного комплекса «Компас»

ФГУП «Научно-технический центр оборонного комплекса «Компас» является издателем следующих научных журналов:

Межотраслевой научно-технический журнал

Оборонный комплекс — научно-техническому прогрессу России
(4 выпуска)

Подписной индекс **79379**

Издается с 1984 года

Межотраслевой научно-технический журнал

Конструкции из композиционных материалов
(4 выпуска)

Подписной индекс **80089**

Издается с 1981 года

Научно-технический журнал

Информационные технологии в проектировании и производстве
(4 выпуска)

Подписной индекс **79378**

Издается с 1976 года

Межотраслевой научно-практический журнал

Экология промышленного производства
(4 выпуска)

Подписной индекс **80090**

Издается с 1993 года

Научно-практический журнал

Вопросы защиты информации
(4 выпуска)

Подписной индекс **79187**

Издается с 1974 года

Все издания ФГУП "Научно-технический центр оборонного комплекса «Компас»:

✓ *включены решением ВАК Министерства образования и науки России в перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата и доктора наук;*

✓ *метаданные выпусков включены в базу данных Российского индекса научного цитирования (РИНЦ).*

Более подробную информацию об изданиях, подписке, дополнительных услугах можно получить по тел.: 8 (495) 491-43-17, 8 (495) 491-77-67, 8 (495) 491-77-20 (*подписка*);
факс: 8 (495) 491-44-80.
E-mail: izdanie@ntckompas.ru

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
«НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР ОБОРОННОГО КОМПЛЕКСА «КОМПАС»
(ФГУП «НТЦ ОБОРОННОГО КОМПЛЕКСА «КОМПАС»)

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

3 (130)

Москва 2020
Основан в 1974 г.

СОДЕРЖАНИЕ

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2020.
Вып. 3 (130). С. 1—56.

Редактор *О. А. Константинова*
Компьютерная верстка: *Н. В. Ильина*, *К. В. Трыкина*

Подписано в печать 27.09.2020. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 6,5. Уч.-изд. л. 6,7.
Тираж 400 экз. Заказ 1958. Свободная цена.
Адрес редакции: 125424, Москва,
Волоколамское ш., 77. ФГУП «НТЦ оборонного комплекса «Компас».
http://ntckompas.ru
Отпечатано в ООО "РАПИТОГРАФ".
117342, Москва, ул. Бутлерова, д. 17Б.
Индекс 79187.

ИНЖЕНЕРНАЯ КРИПТОГРАФИЯ

УДК 621.372.552

Алгоритм сокрытия использования двухкомпонентного контейнера в стеганографической системе

М. В. Шакурский, канд. техн. наук
Самарский государственный технический университет, г. Самара, Россия

Рассмотрен алгоритм формирования двухкомпонентного стеганографического контейнера, позволяющий скрыть встраивание одной из компонент. Это достигается за счет инвариантности двухкомпонентного контейнера относительно маскирующего сигнала.

Ключевые слова: двухкомпонентная стеганографическая система, инвариантность относительно маскирующего сигнала, стеганографический контейнер, растровое изображение, метод наименьших значащих бит.

Формирование заполненного стеганографического контейнера в виде нелинейной функции сигнала пустого контейнера и сообщения значительно повышает устойчивость системы к извлечению скрытого сообщения. Использование двухкомпонентного стеганографического контейнера позволяет извлечь встроенный в контейнер сообщение при неизвестном принимающей стороне сигнале контейнера. В работах [1—10] показано, что при разработке двухкомпонентных стеганографических систем возможно большое количество функций формирования компонент контейнера, включающих как линейные функции, так и нелинейные. Кроме того, функции извлечения скрытого сообщения имеют точку разрыва, вблизи которой наблюдается высокая чувствительность к ошибке в коэффициентах функции.

Известный алгоритм синтеза двухкомпонентного стеганографического контейнера содержит этапы преобразования передаваемого сигнала в два сигнала, формирования двух компонент с помощью маскирующего сигнала и встраивания компонент в контейнер [11]. Для восстановления сообщения необходимы значения двух компонент, передаваемых параллельно или последовательно.

Рассмотрен алгоритм синтеза двухкомпонентного стеганографического контейнера, позволяющий скрыть наличие одной из компонент.

Шакурский Максим Викторович, доцент кафедры "Теоретическая и общая электротехника".
E-mail: M.Shakurskiy@gmail.com

Статья поступила в редакцию 27 июля 2020 г.

Описание алгоритма сокрытия компоненты

Введем следующие термины и обозначения: сообщение — u; передаваемая скрытно информация — u_1 и u_2; встраиваемые сигналы — y_1 и y_2; маскирующий сигнал — ξ; сигнал пустого контейнера — X; сигнал заполненного контейнера, передаваемый по каналу связи, — Y.

Алгоритм сокрытия одной из компонент основывается на свойстве инвариантности функции извлечения сообщения относительно маскирующего сигнала. Так как маскирующий сигнал может быть любым, его синтезируют таким образом, чтобы одна компонента встраиваемого сигнала совпадала с сигналом пустого контейнера.

Математическая модель предложенного алгоритма имеет следующий вид (индексы отсчетов опущены):

$$\begin{cases} y_1 = f(X); \\ u_1 = f(u), \quad u_2 = f(u); \\ \xi = f(y_1, u_1); \\ y_2 = f(u_2, \xi); \\ Y = f(X, y_2). \end{cases} \qquad (1)$$

Технология встраивания сообщения u в контейнер X в соответствии с (1) следующая:

- определяем область контейнера X, соответствующую сигналу y_1, и формируем массив y_1;
- определяем значения u_1 и u_2;
- на основе выбранного метода встраивания сообщения из сигналов y_1 и u_1 определяем маскирующий сигнал ξ;

- формируем вторую компоненту y_2 как функцию маскирующего сигнала ξ и сигнала сообщения u_2;
- определяем область сигнала X для встраивания второй компоненты y_2 и осуществляем встраивание сигнала y_2.

Общая структурная схема стеганографической системы с сокрытием одной компоненты приведена на рис. 1.

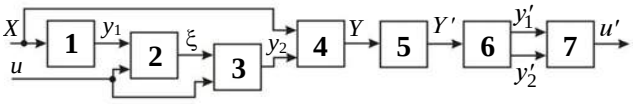


Рис. 1. Структурная схема стеганографической системы

На вход системы подают сигнал пустого контейнера и сигнал сообщения. Подразумевается, что первая компонента y_1 контейнера имеет значение области встраивания сигнала пустого контейнера X. Таким образом, в блоке 1 определяется значение компоненты y_1 как значение соответствующей области сигнала X. Блок 2 определяет значение маскирующего сигнала ξ с помощью выражения для формирования компоненты y_1, значения y_1 и значения сообщения u. Блок 3 формирует значение компоненты y_2 с помощью полученного значения ξ и значения сообщения u в соответствии с алгоритмом формирования y_2. В блоке 4 происходит встраивание второй компоненты y_2 в сигнал X. Сигнал заполненного контейнера Y, получаемый на выходе блока 4, передается на линию связи 5. С линии связи сигнал стеганографического контейнера передается на вход блока выделения компонент 6, откуда поступает на блок стеганографического декодера 7. На выходе декодера 7 формируется извлеченный сигнал сообщения u.

Пример реализации алгоритма сокрытия компоненты

В данном примере реализация алгоритма была проведена для двухбитного сигнала сообщения u. Компоненты y_1 и y_2 занимали три бита информации. Рассматривались два варианта размещения встраиваемых компонент в пространстве контейнера. В примере использовали метод встраивания на основе суммы линейных функций двух сигналов [1]. Математическое описание метода встраивания имеет следующий вид:

$$\begin{cases} y_1 = a_1 + b_1 u_1 + c_1 \xi; \\ y_2 = a_2 + b_2 u_2 + c_2 \xi. \end{cases} \quad (2)$$

С учетом математической модели (1) и структурной схемы (см. рис. 1) математическое описание преобразуется к виду

$$\begin{cases} \xi = \dfrac{y_1 - a_1 - b_1 u_1}{c_1}; \\ y_2 = a_2 + b_2 u_2 + c_2 \xi. \end{cases} \quad (3)$$

Связь между значениями u_1 и u_2 — аддитивная:

$$\begin{aligned} u_1 &= u; \\ u_2 &= K - u_1. \end{aligned} \quad (4)$$

В общем случае методы встраивания могут быть другими.

В одном варианте размещения первая компонента располагалась в области младших бит, в другом варианте — в области старших бит пикселей. На рис. 2 приведено расположение компонент.

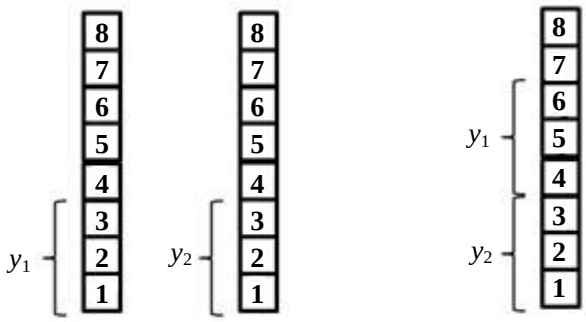


Рис. 2. Размещение встраиваемых компонент:
а — в двух битах контейнера;
б — в одном бите контейнера

На рис. 2, *а* первая компонента располагается в области младших бит одного пикселя, вторая — в области младших бит второго пикселя. Такое расположение позволяет получить следующие результаты.

- Встраивание двух компонент, y_1 и y_2, осуществляется в младшие биты двух пикселей контейнера. При этом первый пиксель сохраняет свое значение яркости. Изменяется только значение младших бит второго пикселя.
- Младшие биты изображений слабо коррелированы, поэтому использование линейного алгоритма встраивания приводит к визуальной неразличимости встроенной информации в области младших бит, а также к искажению плотности распределения вероятности в сторону нормального и к увеличению расстояния Кульбака—Лейблера (встраивание осуществляли непосредственно, без применения каких-либо методов по

улучшению статистических параметров заполненного контейнера).

- Возможны ошибки округления при использовании нелинейных методов встраивания, что требует тщательной подборки коэффициентов выражения (2).

На рис. 2, *б* первая компонента расположена в области старших бит одного пикселя, вторая — в области младших бит того же пикселя.

Такое расположение позволило получить следующие результаты.

- Встраивание двух компонент, y_1 и y_2, осуществляется в пределах одного пикселя. При этом изменяются только младшие биты этого пикселя.
- Старшие биты изображений более коррелированы. Поэтому использование линейного метода встраивания приводит к повышению степени корреляции младших бит изображения. При этом расстояние Кульбака—Лейблера ощутимо увеличивается по отношению к варианту, приведенному на рис. 2, *а*.
- Возможны ошибки округления при использовании нелинейных методов встраивания, что требует тщательной подборки коэффициентов выражения (2).

Заключение

В результате проведенного исследования предложен алгоритм синтеза двухкомпонентного стеганографического контейнера, при использовании которого встраивание одной из компонент не изменяет значения отсчетов пустого контейнера. Алгоритм позволяет увеличить эффективность сокрытия факта встраивания сообщения и значительно повысить устойчивость стеганографической системы к извлечению сообщения. Важным свойством предложенного алгоритма является то, что для извлечения сообщения требуется знание обеих компонент, но определение области скрытой компоненты осложняется тем, что она совпадает с пустым контейнером.

Литература

1. *Шакурский М. В.* Двухкомпонентная стеганографическая система на основе суммы линейных функций двух сигналов, использующая аддитивный вид связи встраиваемых сигналов // Вопросы защиты информации. 2020. № 1(128). С. 10—13.
2. *Шакурский М. В., Козловский В. Н.* Выбор ключа в инвариантных двухкомпонентных стеганографических системах, использующих мультипликативный алгоритм связи встраиваемых сигналов // Проблемы информационной безопасности. Компьютерные системы. 2018. № 4(123). С. 3—9.
3. *Шакурский М. В.* Свойства инвариантных двухкомпонентных стеганографических систем, использующих аддитивный алгоритм связи встраиваемых сигналов // Вопросы защиты информации. 2018. № 4(123). С. 3—9.
4. *Шакурский М. В.* Математические модели двухкомпонентных инвариантных стеганографических систем, использующих различные алгоритмы связи встраиваемых сигналов // Вопросы защиты информации. 2018. № 2(121). С. 8—13.
5. *Шакурский М. В., Шакурский В. К.* Устройство сокрытия информации. Патент 2546307 РФ, МПК H04L 9/00, H04K 3/00. Заявл. 10.06.2014. Опубл. 10.04.2015. Бюл. № 10.
6. *Шакурский М. В., Шакурский В. К.* Способ скрытой передачи информации. Патент 2546306 РФ, МПК H04L 9/00, H04K 3/00. Заявл. 10.06.2014. Опубл. 10.04.2015. Бюл. № 10.
7. *Шакурский М. В.* Устройство сокрытия информации. Патент 167074 РФ, МПК H04L 9/00, H04K 3/00. Заявл. 28.01.2016. Опубл. 20.12.2016. Бюл. № 35.
8. *Шакурский В. К., Шакурский М. В.* Сжимающие отображения в инвариантных преобразователях и системах стеганографии. — Самара: Изд-во СНЦ РАН, 2014.
9. *Шакурский М. В.* Формирование контейнера для стеганографической системы на основе сжимающих отображений // Радиотехника. 2015. № 2. С. 134—139.
10. *Шакурский М. В., Шакурский В. К.* Стеганографическая система на основе сжимающих отображений // Вопросы защиты информации. 2015. № 2. С. 74—78.
11. *Шакурский М. В.* Метод встраивания информации в младшие биты растровых изображений без сжатия, использующий двухкомпонентный контейнер // Вопросы защиты информации. 2020. № 2(129). С. 3—7.

Algorithm for hiding the use of a two-component container in a steganographic system

M. V. Shakurskiy
Samara State Technical University, Samara, Russia

The article discusses an algorithm for forming a two-component steganographic container, which allows to hide the embedding of one of the components. This is achieved due to the invariance of the two-component container from the masking signal.

Keywords: two-component steganographic system, invariance to masking signal, steganographic container, raster image, least significant bit method.

Bibliography 11 references. *Received July 27, 2020*

УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004.056

Моделирование и верификация подсистемы управления доступом средства защиты информации Аккорд-X

[1]*А. М. Каннер*; [1, 2] *Т. М. Каннер*
[1] ЗАО «ОКБ САПР», Москва, Россия
[2] Московский физико-технический институт (национальный исследовательский университет), г. Долгопрудный, Московская обл., Россия

Описана модель управления доступом средства защиты информации Аккорд-X, позволяющего реализовать мандатное управление доступом в операционных системах семейства Linux. В модели учитывается дискреционное управление доступом. Моделирование и верификация модели управления доступом произведены на языке темпоральной логики действий Лэмпорта и соответствующих инструментальных средств верификации.

Ключевые слова: подсистема управления доступом, Аккорд-X, модель безопасности, верификация, темпоральная логика.

Подсистема управления доступом операционной системы представляет собой средство защиты информации (СЗИ), содержащее большой объем исполняемого кода. По мере появления новых требований к таким СЗИ их сложность и объемы исполняемого кода возрастают. Это приводит к появлению новых угроз безопасности и уязвимостей, которые чаще всего связаны с ошибками проектирования средств защиты. Во избежание данной проблемы при разработке подсистем управления доступом любой операционной системы (ОС), в том числе ОС Linux, необходимо предварительно проводить моделирование механизмов защиты. Для этого разрабатывают модели безопасности компьютерных систем [1—3].

Требования к разработке моделей безопасности регламентированы рядом нормативных документов [4—8]. Эти требования предназначены для компаний-разработчиков средств защиты информации. Их выполнение является обязательным при проведении работ по сертификации СЗИ в ФСТЭК России. В соответствии с требованиями нормативных документов в разрабатываемой модели безопасности средств управления доступом должны быть отражены реализуемые политики управления доступом и фильтрации информационных потоков. При этом для подтверждения корректности модели безопасности и тем самым корректности работы СЗИ в части отсутствия логических ошибок в разграничении доступа необходимо подтверждать соответствие модели заявленным требованиям. Наиболее объективным путем подтверждения соответствия модели требованиям является ее верификация с применением специальных инструментальных средств.

Рассмотрим подход к верификации модели безопасности для подсистемы управления доступом, входящей в состав программно-аппаратного комплекса "Аккорд-X" [9, 10] производства компании "ОКБ САПР", а также некоторые особенности процесса верификации.

Материалы и методы

Существует множество подходов к моделированию произвольных систем или алгоритмов в целях их верификации на соответствие некоторым формально описанным свойствам [1—3, 11]. Выбран подход к верификации с использованием темпоральной логики действия Лэмпорта (TLA — Temporal Logic of Actions) и метода Model Checking [1, 2, 12, 13] как наиболее доступный для понимания подход, позволяющий в рамках формальной нотации на языке TLA+ описать все необходимые сущности и операции системы, а также свойства безопасности, необходимые для проверки во всех ее состояниях.

Моделирование на языке темпоральной логики действий Лэмпорта позволяет описывать и в дальнейшем верифицировать в автоматическом режиме системы, заданные в виде конечных автоматов [14]. Вместе с тем при использовании данного

Каннер Андрей Михайлович, программист группы программирования ПО для СЗИ отдела программирования СЗИ.
E-mail: kanner@okbsapr.ru
Каннер Татьяна Михайловна, руководитель учебного центра ЗАО «ОКБ САПР», ведущий инженер лаборатории "Прикладные исследования МФТИ-Сбербанк".
E-mail: tatianash@okbsapr.ru

Статья поступила в редакцию 9 сентября 2020 г.

подхода существуют некоторые ограничения на возможность верификации системы, так как метод Model Checking не осуществляет ее полноценную формальную верификацию. В соответствии с этим в рамках нотации модели безопасности TLA+ введены модельные значения для некоторых сущностей системы (количества субъектов, объектов и пользователей). Такие ограничения на сущности системы, заданные модельными значениями, с одной стороны, не могут повлиять на успешность или неуспешность верификации, а с другой — позволяют методу Model Checking завершить верификацию на этапе, когда для системы не существует новых состояний, т. е. когда все достижимые состояния для данного количества сущностей системы уже проверены. Итак:

* *IDs*
* Множества идентификаторов:
$UserIDs \triangleq 0..2$
$SubjectIDs \triangleq 0..2$
$ObjectIDs \triangleq 0..4$

В модели безопасности необходимо задать переменные — те сущности, которые будут изменяться при выполнении операций и изменение которых влечет за собой изменение состояния системы: A — множество произошедших доступов (вспомогательная переменная [15]); O — множество объектов; S — множество субъектов; U — множество учетных записей пользователей:

VARIABLES A, O, S, U
* Переменные модели:
$vars \triangleq (A, O, S, U)$

Любое изменение приведенных переменных модели переводит систему из одного состояния в другое. Например, во множество произошедших доступов можно добавить новый элемент-кортеж — доступ субъекта с идентификатором *s.sid* к объекту с идентификатором *o.oid* по методу доступа *r* из множества *Accesses*:

$$Accesses \triangleq \left\{ \begin{array}{l} \text{"read", "write", "list\_files", "append",} \\ \text{"lookup", "rename\_obj", "rename\_cont",} \\ \text{"ucreate", "udelete", "change\_user\_perm",} \\ \text{"change\_ext\_attr", "change\_cl", "screate",} \\ \text{"sdelete", "delete\_object","create\_object"} \end{array} \right\}$$

$$A' = A \cup \{< s.sid,\ o.oid,\ r >\}$$

Изменение тех или иных переменных модели необходимо описывать в операциях, которые можно выполнить в системе, соответствующих методам доступа *Accesses*: чтение, запись, получение содержимого каталога, дозапись, поиск объекта, переименование объектов и контейнеров, создание и удаление пользователей, изменение прав пользователей, изменение атрибутов и уровня конфиденциальности объектов доступа, создание и удаление субъектов (процессов пользователей), удаление и создание объектов доступа.

Все операции в нотации TLA+ описывают в виде предикатов пред- и постусловий выполнения операции, например:

* Read
* Операция чтения:
$Read\ (s,o) \triangleq$
$\quad \wedge A' = A \cup \{\langle s.sid,\ o.oid,\ \text{"read"}\rangle\}$
$\quad \wedge$ UNCHANGED $\langle S, O, U\rangle$
$Read\ D \triangleq$
$\exists s \in S:$
$\exists o \in O:$

* Проверка прав
$\wedge \vee\ IsUserAdmin(s)$
* *DAC*
$\vee \wedge\ DAC\_may\_do\ (s, o, \text{"read"})$
* *MAC*
$\quad \wedge MAC\_may\_read\ (s, o)$
* Lookup
$\wedge \langle s.sid, o.oid, \text{"}lookup\text{"}\rangle \in A$
* Постусловия
$\wedge\ Read\ (s,o)$

В предусловии *ReadD* описано несколько предикатов, соединенных операторами конъюнкции (логическое И) и дизъюнкции (логическое ИЛИ). Смысл данного предусловия можно трактовать следующим образом: должны существовать субъект и объект, такие, что одновременно выполняются условия:

- либо субъект является администратором, либо должны одновременно быть выполнены свойства дискреционной и мандатной политик управления доступом (предикаты *DAC_may_do* и *MAC_may_read*);
- субъектом должен быть предварительно выполнен поиск объекта доступа.

В постусловии *Read (s, o)* изменяется переменная с произошедшими доступами системы, а остальные переменные модели остаются неизменными.

Предикаты *isUserAdmin*, *DAC_may_do* и *MAC_may_read* реализованы следующим образом.

* Предикаты проверки дискреционного
* управления доступом:

$$IsUser\ Admin(s) \triangleq$$
$$\wedge\ SelectUser(s.uid).is\_admin = \text{TRUE}$$
$$\backslash^*\ a \in Permissions$$
$$DAC\_may\_do(s, o, a) \triangleq$$
$$\wedge\ \exists\ r \in SelectUser(s.uid).acls:$$
$$\wedge\ r[1] = o.oid$$
$$\wedge\ a \in r[2]$$

* Предикаты проверки мандатного
* управления доступом:

$$MAC\_may\_read(s, o) \triangleq$$
$$\vee\ o.cl \le s.cl$$
$$\vee\ \text{"ccnr"} \in o.ext\_attr$$

Здесь *cl* — уровень доступа субъекта или конфиденциальности объекта;

ccnr — специальный атрибут, позволяющий для объекта делать исключение в рамках мандатной политики управления доступом [3].

Аналогичным образом в нотации модели безопасности TLA+ описаны все остальные операции, соответствующие методам доступа *Accesses*, с учетом характерных для них ограничений, в том числе дискреционного и мандатного управления доступом.

Начальное состояние системы описывается с помощью следующего предиката:

* *Init*
* Инициализация:

$$Init \triangleq\ \wedge A = \{\ \}$$
$$\wedge S = \{s0, s1\}$$
$$\wedge O = \{o0,\ o1,\ o2\}$$
$$\wedge U = \{u0,\ u1\}$$

Множество произошедших доступов инициализируется пустым. В системе изначально существуют две учетные записи пользователей: *u*0 — администратор с максимальным уровнем конфиденциальности и *u*1 — модельный пользователь с минимальным уровнем конфиденциальности, а также соответствующие им субъекты-процессы *s*0 и *s*1 и объекты — корневой каталог файловой системы *o*0, вложенный контейнер *o*1 и файл этого контейнера *o*2. Данные модельные сущности выбраны для ускорения процесса верификации. Множество объектов или субъектов может изначально быть пустым, но это приведет к значительно большему количеству состояний системы.

Условия или свойства безопасности, которые необходимо описывать и проверять в рамках нотации TLA+, представляют в виде инвариантов или темпоральных свойств [12, 13]. При этом в рамках данной модели безопасности за счет использования переменной истории (*history variable* [15]) для множества всех совершенных доступов нет необходимости использовать темпоральные свойства, которые, в отличие от инвариантов, зависят от фактора времени и событий в прошлом или будущем. Все свойства безопасности описаны как предикаты, истинность которых проверяется в каждом возможном состоянии системы.

Для модели описаны инварианты: проверяющие правильность функционирования системы и инварианты безопасности. Первой группе принадлежат инварианты *TypeInv* (консистентность типов сущностей системы), *OneAdminExists* (существование в любой момент администратора системы), *NoCyclesInContainers* (отсутствие циклов в контейнерах). К инвариантам безопасности относятся *MacSafety* (невозможность существования вложенного в контейнер объекта с большим уровнем конфиденциальности), *IntegrityInv* (невозможность запуска измененных исполняемых файлов), *LinksSafety* (наследование уровня конфиденциальности всех ссылок от уровня объекта доступа).

* *MACSafety*
* Инвариант безопасности мандатного
* управления доступом для иерархии объектов
* в контейнере:

$$MACSafety \triangleq$$
$$\forall\ o \in O:$$
$$\vee\ \wedge\ o.type \in Containers$$
$$\wedge\ \forall\ ch \in SelectAllChilds(o):$$
$$\wedge\ \vee\ ch.cl \le o.cl$$
$$\vee\ \text{"ccnr"} \in o.ext\_attr$$
$$\vee\ \neg\ o.type \in Containers$$

* *IntegrityInv*
* Инвариант динамического контроля
* целостности:

$$IntegrityInv \triangleq \forall\ e \in Select\ Executables:$$
$$\left(SubjectIDs \times \{e.oid\} \times \{\text{"write", "append"}\}\right) \cap A = \{\}$$

Модель безопасности в нотации TLA+ описана с помощью спецификации *Spec*, для которой зада-

но начальное состояние *Init* и в дальнейшем могут выполняться различные действия из *Next*.

* *Spec*
* Спецификация модели:

$$Spec \triangleq Init \wedge \Box [Next]_{vars}$$

* Invariants
* Теорема, учитывающая все инварианты
* (доказывается в процессе верификации):

$$\begin{aligned} \text{THEOREM } Spec \Rightarrow & \wedge \Box\, TypeInv \\ & \wedge \Box\, OneAdminExists \\ & \wedge \Box\, MACSafety \\ & \wedge \Box\, NoCyclesInContainers \\ & \wedge \Box\, IntegrityInv \\ & \wedge \Box\, LinksSafety \end{aligned}$$

Формальное доказательство отсутствия противоречий в модели безопасности осуществляют с помощью проверки в автоматическом режиме рассмотренных инвариантов в каждом возможном состоянии для спецификации *Spec*.

Результаты

Верификацию разработанной модели проводили с помощью инструментального средства TLC2 v2.15 на СВТ с Intel Core i5-9400 (3,80 ГГц) и объемом оперативной памяти 16 ГБ в 64-разрядной ОС Linux с ядром v5.4.38. Время, затраченное на верификацию с использованием 6 отдельных потоков, составляет от 12 мин до 24 ч в зависимости от выставленных опций верификации — проверки модели с итеративным углублением, начиная с заданной глубины (опция *dfid* от 6 до 8). Общее количество различных проанализированных состояний 2 776 895.

Результаты верификации описанной спецификации относительно заданных инвариантов позволяют сделать вывод о выполнении требований безопасности для всех возможных состояний модели управления доступом.

Верификация модели позволила выявить и устранить недостатки в реализации комплекса "Аккорд-X", а также провести дальнейший анализ возможных скрытых каналов утечки информации при реализации мандатного управления доступом.

Заключение

Рассмотрен подход, использованный в процессе верификации модели безопасности для подсистемы управления доступом комплекса "Аккорд-X". Данный подход не только позволил выполнить формальные требования существующих нормативных документов в области защиты информации, но и способствовал выявлению логических ошибок в работе подсистемы разграничения доступа, которые могли привести к нарушению конфиденциальности или целостности защищаемых данных.

Литература

1. *Козачок А. В.* Спецификация модели управления доступом к разнокатегорийным ресурсам компьютерных систем // Вопросы кибербезопасности. 2018. № 4(28). С. 2—8.
2. *Козачок А. В.* Спецификация модели управления доступом на языке темпоральной логики действий Лэмпорта // Тр. Института системного программирования РАН. 2018. Т. 30. № 5. С. 147—162.
3. *Девянин П. Н. и др.* Моделирование и верификация политик безопасности управления доступом в операционных системах. — М.: Горячая линия-Телеком, 2019. — 212 с.
4. *Мозолина Н. В.* Формальное моделирование политики безопасности: к вопросу о стандартизации процесса // Комплексная защита информации. 2019. С. 96—99.
5. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка). [Приказ ФСТЭК России от 30 июля 2018 г. № 131]. — М.: ФСТЭК России, 2018. — 17 с.
6. ГОСТ Р ИСО/МЭК 15408-3-2013 Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Компоненты доверия к безопасности. — М.: Стандартинформ, 2014. — 152 с.
7. ГОСТ Р (проект) Защита информации. Формальное моделирование политики безопасности. Ч. 1. Формальная модель управления доступом. — М.: Стандартинформ, 201х. — 36 с.
8. ГОСТ Р (проект) Защита информации. Формальное моделирование политики безопасности. Ч. 2. Верификация формальной модели управления доступом. — М.: Стандартинформ, 201х. — 36 с.
9. *Каннер А. М., Ухлинов Л. М.* Управление доступом в ОС GNU/Linux // Вопросы защиты информации. 2012. № 3. С. 35—38.
10. *Каннер А. М.* Linux: о жизненном цикле процессов и разграничении доступа // Вопросы защиты информации. 2014. № 4. С. 37—40.
11. *Klein G. et al.* seL4: formal verification of an OS kernel // Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles. 2009. P. 207—220. DOI: https://doi.org/10.1145/1629575.1629596
12. *Lamport L.* The Temporal Logic of Actions // ACM Trans. Program. Lang. Syst. 1994. V. 16. № 3. P. 872—923. DOI: http://doi.acm.org/10.1145/177492.177726
13. *Lamport L. et al.* Specifying and verifying systems with TLA+ // Proceedings of the ACM SIGOPS 10th workshop. 2002. P. 45—48.
14. *Kanner A. M., Kanner T. M.* Testing Software and Hardware Data Security Tools Using the Automata Theory and the Graph Theory // Proceedings of Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology. 2020. P. 615—618.
15. *Lamport L., Merz S.* Auxiliary variables in TLA+ [Электронный ресурс]. URL: https://arxiv.org/pdf/1703.05121.pdf (дата обращения: 01.09.2020).

Modeling and verification of the access control subsystem of Accord-X data security tool

[1]*A. M. Kanner,* [1, 2] *T. M. Kanner*
[1] JSC "OKB SAPR", Moscow, Russia
[2] Moscow Institute of Physics and Technology (National Research University), Dolgoprudny, Moscow region, Russia

The article describes the access control model of the Accord-X data security tool, which makes it possible to implement mandatory access control in the Linux operating systems. The model also takes into account discretionary access control. Modeling and verification of the access control model was carried out in the language of Lamport's temporal logic of actions and the corresponding verification tools.

Keywords: access control subsystem, Accord-X, security model, verification, temporal logic.

Bibliography — 15 references. *Received September 9, 2020*

УДК 004.056

Реализация концепции управления конфигурациями при помощи программного модуля "Паспорт ПО"

Н. В. Мозолина
Московский физико-технический институт (государственный университет),
г. Долгопрудный, Московская обл., Россия

Рассмотрены основные принципы концепции управления конфигурациями, ориентированного на безопасность. Продемонстрирована возможность реализации этих принципов при решении задачи контроля конфигурации рабочих мест пользователей при помощи программного модуля "Паспорт ПО".

Ключевые слова: управление конфигурациями, контроль конфигурации, администрирование.

Авторы различных научных статей [1, 2] и учебников [3—5] по защите информации, специалисты компаний, разрабатывающих системы безопасности [6], едины в вопросе построения систем защиты. Их создание начинают с анализа текущего состояния информационной системы (ИС), для которой разрабатывают защиту, с определения объектов защиты, а также с построения модели угроз. Завершающим этапом является сопровождение разработанной системы, т. е. ее непрерывный мониторинг, контроль состояния и конфигураций, причем этот контроль необходимо осуществлять в течение всей жизни ИС вплоть до ее ликвидации. Указанный подход к построению систем защиты нашел свое отражение и в национальном стандарте [7], а в концепции управления конфигурациями, ориентированного на безопасность (Security-Focused Configuration Management of Information Systems, SecCM) [8], приведены основные принципы, позволяющие организовать повышение защищенности информационной системы за счет управления ее конфигурациями.

Изучим методы контроля состояния рабочих мест пользователя, а также рассмотрим особенности этого контроля при помощи программного модуля (ПМ) "Паспорт ПО" [9] с точки зрения повышения защищенности системы.

Материалы и методы

Для большинства информационных систем характерны постоянные изменения в результате установки нового программного и аппаратного обеспечения, его обновления или удаления, создания документов, баз данных и т. д. Конфигурация системы и ее компонентов оказывает прямое влияние на состояние безопасности. Изменения, происходящие на рабочих местах пользователей, могут быть как результатом санкционированных действий (например, обновление версии программных модулей администратором), так и результатом работы некоторого вредоносного программного обеспечения (ПО), случайного или намеренного внесения нежелательных изменений пользователем.

Последствиями несанкционированных изменений могут быть нерациональное использование рабочего времени за счет использования служебных компьютеров в личных целях, угрозы безопасности и промышленный шпионаж из-за установки пользователями потенциально или заведомо опасных программ и даже полное нарушение работоспособности системы [9].

Для своевременного обнаружения и предотвращения таких изменений недостаточно организационных мер (инструкций, регламентов), необходим постоянный мониторинг состояния рабочих мест пользователя. Обеспечить такой контроль может программный модуль "Паспорт ПО" (ПМ "Паспорт ПО"), разработанный для анализа программной среды компьютеров под управлением ОС Windows.

Рассмотрим применение ПМ "Паспорт ПО" и покажем, как его функциональные возможности позволяют реализовать ключевые принципы управления конфигурациями, ориентированного на безопасность. Проанализируем данные, полученные из литературных источников, проведем аналогию между изученными возможностями.

Мозолина Надежда Викторовна, аспирант.
E-mail: mozolina@phystech.edu

Статья поступила в редакцию 22 сентября 2020 г.

Результаты изучения материалов и методов

Управление конфигурациями, ориентированное на безопасность, — одна из концепций повышения защищенности информационной системы за счет управления ее конфигурациями. Реализация принципов SecCM заключается в:

- идентификации и записи конфигураций, которые влияют на состояние безопасности системы и организации;
- учете рисков безопасности при утверждении начальной конфигурации;
- анализе последствий изменения конфигурации системы для безопасности;
- документировании одобренных и внедренных изменений [8].

Важность управления конфигурациями, ориентированного на безопасность, заключается в возможности с его помощью сократить время обнаружения компрометации компонента информационной системы, уменьшить влияние атаки за счет ее раннего обнаружения, снизить принесенный ущерб [10, 11].

В [8] указаны основные действия, выполнение которых позволяет реализовать корректное управление конфигурациями в информационной системе. Так, ключевыми этапами являются планирование SecCM (разработка политик применения средства SecCM), внедрение SecCM (определение базовых конфигураций и их утверждение), контроль изменений конфигурации (использование некоторой панели управления конфигурации для рассмотрения и утверждения изменений в ИС) и мониторинг уже утвержденных конфигураций.

ПМ "Паспорт ПО" предназначен для автоматизации контроля целостности состояния программной среды (основных характеристик файлов программного обеспечения) и контроля изменений состава ПО (установленные на средство вычислительной техники системные и прикладные программные продукты). Назовем конфигурацией СВТ программную среду вместе с совокупностью состава ПО. Фиксацию состояния конфигурации СВТ выполняют через создание записей специального вида — проектов паспортов ПО. Заверенный (подписанный электронной подписью) проект паспорта называют паспортом ПО. Он представляет эталонное состояние конфигурации СВТ. Для формирования паспорта ПО пользователь должен обладать в рамках ПМ "Паспорт ПО" правом на подпись проекта.

Основными элементами ПМ "Паспорт ПО" являются:

- серверный компонент (Сервер) с базой данных;
- компонент управления (АРМ управления);
- клиентский компонент (Клиент), устанавливаемый на подконтрольные объекты (ПКО), рабочие места (СВТ), конфигурацию которых контролирует программный модуль;
- сервис обмена сообщениями RabbitMQ, обеспечивающий взаимодействие по сети между всеми элементами [12].

Подготовка системы для работы ПМ "Паспорт ПО" заключена в выполнении следующих действий:

- регистрация учетных записей административного персонала, отвечающего за контроль целостности программной среды в АРМ управления, формирование ролей и назначение их учетным записям;
- формирование списка ПКО с разбиением на логические группы (подразделения);
- формирование общей базы шаблонов (прототипов конфигураций рабочих мест пользователей);
- назначение шаблонов подконтрольным объектам;
- проведение опроса на ПКО (сканирования конфигурации СВТ в соответствии с назначенным шаблоном) и формирование его паспорта ПО.

Покажем, что указанные действия могут быть рассмотрены как выполнение этапов планирования SecCM и внедрения SecCM.

В результате подготовки системы в базе данных ПМ "Паспорт ПО" формируются записи об эталонном состоянии конфигурации СВТ с установленным Клиентом. В ходе дальнейшей работы выполняют сканирование подконтрольных объектов по заданному для СВТ расписанию или по запросу управляющего персонала ПМ "Паспорт ПО". В ходе сканирования Клиент определяет конфигурацию СВТ и отправляет информацию на Сервер, который автоматически сверяет полученные данные о текущем состоянии ПКО с эталонным и информирует управляющий персонал ПМ "Паспорт ПО" о выявленных нарушениях. Для каждого ПКО в случае обнаружения нарушений должен быть выполнен анализ возникших изменений, в результате которого возможны обновление паспорта ПО в случае санкционированных модификаций или же принятие мер по устранению причин возникших несоответствий, разбор инцидента безопасности. Данные операции являются третьим этапом реализации SecCM.

Информацию обо всех действиях по формированию как проектов паспортов ПО, так и самих паспортов ПО сохраняют в журнале событий ПМ "Паспорт ПО". Анализ сообщений из журнала событий позволяет производить выявление изменений в уже утвержденных паспортах, реализуя тем самым этап мониторинга SecCM.

Рассмотрев основные функции ПМ "Паспорт ПО" и сопоставив этапы его применения с этапами реализации концепции SecCM, выполним сравнение основных процессов и объектов, на которые опирается стандарт SecCM [8, с. 17, 18], и процессов и объектов, которыми оперирует программный модуль. Результат такого сравнения представлен в таблице.

Обсуждение

Приведенное сопоставление, а также соответствие между этапами SecCM и этапами применения ПМ "Паспорт ПО" показывает, что программный модуль может быть рассмотрен как средство, реализующее управление конфигурациями, ориентированное на безопасность.

Стоит отметить, что рассмотренный ПМ "Паспорт ПО" является наложенным средством контроля изменений рабочих мест пользователя.

В то же время использование большого числа компьютеров под управлением ОС Windows почти всегда сопровождается их объединением с использованием службы каталогов Active Directory (AD) в единый домен.

Эта служба позволяет управлять различными объектами (рабочими компьютерами, серверами, принтерами, пользователями и т. д.) из единой точки (контролера домена), а также получать сведения о состоянии объектов и об их изменениях [13], т. е. выполнять мониторинг конфигураций.

Итак, мы сталкиваемся с необходимостью наложенного средства даже при условии, что в системе есть встроенная система с аналогичной функциональностью.

Результаты сравнения процессов

NIST.SP.800-128	ПМ "Паспорт ПО"
Управление конфигурацией (Configuration Management — CM) — набор действий, направленных на создание и поддержание целостности продуктов и систем посредством контроля процессов создания, изменения и мониторинга конфигураций этих продуктов и систем	Набор действий по формированию базы шаблонов (типовых конфигураций СВТ), назначению их рабочим местам пользователей, формированию паспортов ПО, проведению сканирования рабочих мест и сравнению текущей конфигурации СВТ (проекта паспорта) с эталонной (паспорт ПО)
Элемент конфигурации (Configuration Item — CI) — идентифицируемая часть системы (например, аппаратное обеспечение, программное обеспечение, встроенное ПО, документация или их комбинация), которая является дискретной целью процесса управления конфигурацией	Подконтрольный объект (ПКО) — СВТ с установленным на него Клиентом ПМ "Паспорт ПО" — однозначно идентифицируется именем ПКО. Обеспечение контроля целостности конфигурации ПКО является целью применения ПМ "Паспорт ПО"
Базовая конфигурация (Baseline Configuration) — набор спецификаций для системы или элемента конфигураций в системе, который был рассмотрен и согласован в определенный момент времени и который может быть изменен только через процедуры контроля изменений	Паспорт ПО — заверенный проект паспорта ПО, содержащий информацию о конфигурации СВТ. Процесс заверения проекта заключается в его подписи пользователем ПМ "Паспорт ПО". Формирование нового паспорта ПО для СВТ возможно лишь в результате формирования нового проекта паспорта ПО, его сопоставления с действующим паспортом, а также подписи данного проекта
План управления конфигурацией (Configuration Management Plan — CM Plan) — полное описание ролей, обязанностей, политики и процедуры, применяемых при управлении конфигурацией продуктов и системы	ПМ "Паспорт ПО" является инструментом контроля целостности состояния программной среды. Регламент его применения для мониторинга конфигураций рабочих мест пользователей информационной системы может быть рассмотрен как план управления конфигурацией

Хотя использование встроенных в AD технологий позволяет осуществлять контроль изменений рабочих мест, применение данной службы каталогов порождает "проблему суперпользователя", т. е. сосредоточения максимальных привилегий в рамках одной роли (в данном случае — в рамках роли администратора домена). Обладая полными правами, пользователь с указанной ролью может вносить любые изменения, что делает бессмысленным возложение на него обязанностей по контролю этих изменений и требует создания отдельных учетных записей с усеченной ролью для мониторинга. Создание для пользователей учетных записей, назначение учетным записям ролей может выполнять администратор домена. В то же время это нарушает концепцию разделения ролей администратора и администратора информационной безопасности (ИБ).

Аналогично использованию ПАК "Сегмент-В" для управления доступом в виртуальной инфраструктуре VMware vSphere [14] применение наложенного средства контроля изменений позволяет избежать "проблемы суперпользователя", а также смешения прав и обязанностей администратора и администратора ИБ.

Таким образом, наложенное средство контроля хотя частично и дублирует встроенную функциональность, но является необходимым компонентом защищенной информационной системы.

Заключение

При построении системы защиты некоторой ИС следует помнить, что данный процесс не завершается вводом средств защиты информации в эксплуатацию, их настройкой. Контроль состояния и конфигурации каждого элемента должен выполняться в течение всей жизни информационной системы. Для выполнения этого контроля необходим комплексный подход: как разработка различных регламентов по порядку внесения изменений, так и применение автоматизированных средств контроля конфигураций. Программный модуль "Паспорт ПО" позволяет решить задачу контроля изменений конфигурации рабочих мест пользователей, реализуя принципы управления конфигурациями, ориентированного на безопасность.

Литература

1. *Селищев В. А., Чечуга О. В., Наседкин М. Н.* Построение системы информационной безопасности предприятия // Изв. ТулГУ. Технические науки. 2009. № 1, 2 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/postroenie-sistemy-informatsionnoy-bezopasnosti-predpriyatiya (дата обращения: 13.08.2020).
2. *Гудков С. Н., Коробкин Д. И., Рогозин Е. А.* Основные этапы и задачи проектирования программных систем защиты информации в автоматизированных системах // Вестник ВГТУ. 2009. № 10 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/osnovnye-etapy-i-zadachi-proektirovaniya-programmnyh-sistem-zaschity-informatsii-v-avtomatizirovannyh-sistemah (дата обращения: 05.09.2020).
3. *Внуков А. А.* Защита информации в банковских системах: учебное пособие для бакалавриата и магистратуры. Изд. 2-е, испр. и доп. — М: Юрайт, 2018. — 246 с.
4. *Ясенев В. Н.* Конспект лекций по информационной безопасности [Электронный ресурс]. URL: http://www.iee.unn.ru/wp-content/uploads/sites/9/2017/02/konspekt-lektsij-po-IB.pdf С. 110-112 (дата обращения: 05.09.2020).
5. *Гришина Н. В.* Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.
6. Создание системы защиты персональных данных, приведение процессов обработки и обеспечения безопасности персональных данных в соответствие требованиям законодательства [Электронный ресурс]. URL: https://www.dialognauka.ru/services/creation_system_security_personal_data/ (дата обращения: 13.09.2020).
7. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
8. Guide for Security-Focused Configuration Management of Information Systems [Электронный ресурс]. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf (дата обращения: 13.09.2020).
9. Сайт компании ОКБ САПР. Паспорт ПО [Электронный ресурс]. URL: https://www.okbsapr.ru/products/management/software-passport/ (дата обращения: 05.09.2020).
10. *Jackson B.* Why Security Configuration Management (SCM) Matters [Электронный ресурс]. URL: https://www.tripwire.com/state-of-security/security-data-protection/security-configuration-management/why-security-configuration-management-matters/ (дата обращения: 13.09.2020).
11. *Crast F.* NIST issues Security-Focused Configuration Management Guidelines [Электронный ресурс]. URL: https://www.securezoo.com/2019/11/nist-issues-security-focused-configuration-management-guidelines/ (дата обращения: 13.09.2020).
12. Программный модуль автоматизированного форматирования паспортов программного обеспечения автоматизированных рабочих мест и серверов "Паспорт ПО". Общее описание 11443195.501410.080 94 [Электронный ресурс]. URL: https://www.okbsapr.ru/upload/iblock/ecb/ecbafca5423510fd018bc3e32c6b8c9a.pdf
13. Active Directory Domain Services Overview [Электронный ресурс]. URL: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (дата обращения: 13.09.2020).
14. *Угаров Д. В., Постоев Д. А.* Проблемы реализации разграничения доступа к функциям управления виртуальных сред // Вопросы защиты информации. 2016. Вып. 3. № 114. С. 34, 35.

Implementation of the configuration management concept using the software module "Passport PO"

N. V. Mozolina
Moscow Institute of Physics and Technology (State University),
Dolgoprudny, Moscow region, Russia

The article discusses the basic principles of the concept of Security-Focused Configuration Management of Information Systems as well as the possibility of their implementation to control the configuration of working met users using the software module "Passport PO".

Keywords: configuration management, configuration control, administration.

Bibliography — 14 references. *Received September 22, 2020*

ЭЛЕКТРОННАЯ ПОДПИСЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 003.26

Альтернативный способ построения схем цифровой подписи, удовлетворяющих критерию постквантовой стойкости

А. А. Костина; Н. А. Молдовян, д-р техн. наук
Санкт-Петербургский Федеральный исследовательский центр РАН, Санкт-Петербург, Россия

В целях сокращения размеров открытого ключа и подписи предложен новый способ построения схем электронной цифровой подписи на основе скрытой задачи дискретного логарифмирования, удовлетворяющих ранее сформулированному критерию постквантовой стойкости, требующему устранения периодов, связанных со значением дискретного логарифма, в периодических функциях, задаваемых по открытым параметрам криптосхемы. На основе данного способа разработана схема цифровой подписи, базовым примитивом которой является операция экспоненцирования в скрытой коммутативной группе, обладающей двухмерной цикличностью. В качестве алгебраического носителя криптосхемы использована восьмимерная конечная некоммутативная ассоциативная алгебра, содержащая достаточно большое число различных групп с двухмерной цикличностью. Открытый ключ представляет собой три восьмимерных вектора, вычисляемых в зависимости от двух векторов простого порядка, образующих базис скрытой коммутативной группы. Цифровая подпись представляет собой три 256-битовых числа.

Ключевые слова: защита информации, криптография, электронная цифровая подпись, постквантовая криптосхема, задача дискретного логарифмирования, конечная ассоциативная алгебра, некоммутативная алгебра.

Одно из перспективных направлений в области криптографии представляет собой разработка постквантовых двухключевых алгоритмов и протоколов [1, 2], в частности схем электронной цифровой подписи (ЭЦП). Перспективным подходом к построению практичных постквантовых схем ЭЦП является использование конечных некоммутативных ассоциативных алгебр (КНАА) в качестве алгебраического носителя и скрытой задачи дискретного логарифмирования (СЗДЛ) в качестве базового криптографического примитива [3—6]. Применение СЗДЛ обосновано тем, что периодические функции, задаваемые по открытым параметрам схемы ЭЦП, принимают значения из многочисленных циклических групп, содержащихся в алгебраическом носителе как подмножества его элементов. Последнее устраняет квантовые атаки (атаки с использованием квантового компьютера), основанные на применении известных полиномиальных по времени квантовых алгоритмов вычисления длины периодов, которые применимы для периодических функций, принимающих значения в фиксированной конечной циклической группе [7—9].

Поскольку в первых схемах ЭЦП, основанных на СЗДЛ, имеется возможность задания периодических функций, содержащих период, связанный со значением дискретного логарифма, актуален вопрос о потенциальной возможности разработки новых квантовых алгоритмов вычисления длины периода для общего случая периодических функций, принимающих значения в КНАА. При появлении таких квантовых алгоритмов упомянутые схемы ЭЦП перестанут быть стойкими. В связи с этим в работе [10] для построения схем ЭЦП, основанных на СЗДЛ, предложен следующий общий критерий постквантовой стойкости: *на основе использования открытых параметров схемы ЭЦП должно быть вычислительно невозможно задать периодическую функцию, содержащую период, зависящий от значения дискретного логарифма*.

При выполнении этого критерия конструируемая схема ЭЦП будет стойкой к квантовым атакам как на основе известных, так и на основе потенциально возможных новых квантовых алгоритмов вычисления длин периодов периодических функций. В [10] предложена идея использования коммутативной группы с двухмерной цикличностью (порождаемой базисом из двух элементов, обладающих одинаковыми значениями порядка, см., например, [11]) и формирования открытого ключа

Костина Анна Александровна, научный сотрудник.
E-mail: anna1805@mail.ru
Молдовян Николай Андреевич, профессор, главный научный сотрудник.
E-mail: nmold@mail.ru

Статья поступила в редакцию 3 августа 2020 г.

в виде двух векторов путем маскирования двух элементов скрытой группы, принадлежащих различным циклическим группам. Однако предложенный в [10] способ требует удвоения проверочного соотношения, формирования дополнительного открытого ключа и использования дополнительного элемента ЭЦП в виде вектора. Последнее приводит к существенному увеличению длины подписи (в 3 раза и более).

Предлагаем новый способ построения схем ЭЦП, основанных на СЗДЛ и удовлетворяющих общему критерию постквантовой стойкости, и новую схему ЭЦП, в которой в качестве скрытой группы использована коммутативная группа с двухмерной цикличностью.

Используемый алгебраический носитель

Для построения схем ЭЦП, удовлетворяющих общему критерию постквантовой стойкости, использован алгебраический носитель в виде КНАА, содержащей достаточно большое число различных коммутативных групп с двухмерной цикличностью. Рассмотрим понятие КНАА. Пусть дано m-мерное векторное пространство, которое задано над конечным полем $GF(p)$. Некоторый вектор $\mathbf{A}$ будем записывать в виде упорядоченного набора значений из $GF(p)$, называемых координатами вектора: $\mathbf{A} = (a_0, a_1, \ldots, a_{m-1})$. В отдельных случаях удобнее представлять вектор в виде $\mathbf{A} = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, где $\mathbf{e}_i$ — базисные векторы; $a_i\mathbf{e}_i$ — одномерные компоненты вектора $\mathbf{A}$; $a_i \in GF(p)$ — координаты вектора. Векторное пространство с дополнительно заданной операцией векторного умножения произвольной пары векторов, дистрибутивной слева и справа относительно операции сложения, называют алгеброй.

Операция векторного умножения векторов $\mathbf{A} = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$ и $\mathbf{B} = \sum_{j=0}^{m-1} b_j \mathbf{e}_j$ определяется как перемножение каждой компоненты вектора $\mathbf{A}$ и каждой компоненты вектора $\mathbf{B}$, выполняемое в соответствии с формулой

$$\mathbf{A} \circ \mathbf{B} = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j \left(\mathbf{e}_i \circ \mathbf{e}_j \right),$$

в которой все произведения пар базисных векторов заменяют на соответствующие однокомпонентные векторы, т. е. каждое из произведений $\mathbf{e}_i \circ \mathbf{e}_j$ заменяют на некоторый вектор $\lambda\,\mathbf{e}_k$, выбираемый по специально заданному правилу, представляемому, например, в виде таблицы умножения базисных векторов (ТУБВ). В случае $\lambda = 1$ в ТУБВ указывают базисный вектор $\mathbf{e}_k$. Если значение λ не равно единице, то его называют структурным коэффициентом. Выбор значений $\lambda\,\mathbf{e}_k$ осуществляют следующим образом. В произведении $\mathbf{e}_i \circ \mathbf{e}_j$ первый (левый) операнд указывает строку, а второй (правый) — столбец, на их пересечении получаем ячейку, содержащую требуемое значение $\lambda\,\mathbf{e}_k$.

Для задания ассоциативной алгебры разрабатывают ТУБВ, которая определяет операцию векторного умножения (далее называемую просто операцией умножения), обладающую свойством ассоциативности, т. е. такую операцию умножения, для которой для всевозможных троек векторов $\mathbf{A}$, $\mathbf{B}$ и $\mathbf{C}$ имеет место равенство

$$(\mathbf{A} \circ \mathbf{B}) \circ \mathbf{C} = \mathbf{A} \circ (\mathbf{B} \circ \mathbf{C}).$$

В случае, если равенство $\mathbf{A} \circ \mathbf{B} = \mathbf{B} \circ \mathbf{A}$ выполняется для произвольной пары векторов $\mathbf{A}$ и $\mathbf{B}$, операцию умножения и задаваемую алгебру называют коммутативными, в противном случае — некоммутативными (тогда имеем КНАА).

В качестве алгебраического носителя рассматриваемой далее схемы ЭЦП используем восьмимерную КНАА, заданную по табл. 1 [10], в которой содержатся коммутативные группы с двухмерной цикличностью. Задать базис некоторой группы такого вида достаточно легко. В качестве структурного коэффициента λ выберем элемент поля $GF(p)$, являющийся квадратичным вычетом в $GF(p)$.

Таблица 1

ТУБВ для задания восьмимерной КНАА [10] ($\lambda \neq 1$; $\sigma \neq 0$; $\sigma \neq 1$)

∘	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\sigma\mathbf{e}_6$	$\sigma\mathbf{e}_7$	$\sigma\mathbf{e}_0$	$\sigma\mathbf{e}_1$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\sigma\mathbf{e}_7$	$\sigma\lambda\mathbf{e}_6$	$\sigma\mathbf{e}_1$	$\sigma\lambda\mathbf{e}_0$	$\mathbf{e}_7$	$\lambda\mathbf{e}_6$
$\mathbf{e}_2$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\sigma\mathbf{e}_2$	$\sigma\mathbf{e}_3$	$\sigma\mathbf{e}_4$	$\sigma\mathbf{e}_5$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\sigma\mathbf{e}_3$	$\sigma\lambda\mathbf{e}_2$	$\sigma\mathbf{e}_5$	$\sigma\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$
$\mathbf{e}_6$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_6$	$\mathbf{e}_7$
7	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_7$	$\lambda\mathbf{e}_6$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_7$	$\lambda\mathbf{e}_6$

Конечные группы с многомерной цикличностью

В множестве коммутативных конечных групп выделяют подмножество групп с многомерной цикличностью [11, 12]. Для раскрытия последнего термина используем понятие базиса группы. Базис группы представляет собой минимальный по численности набор элементов группы, всевозможные произведения степеней которых пробегают (принимают) все значения в группе. Конечной группой с μ-мерной цикличностью называют группу, в которой все элементы базиса имеют одинаковое значение порядка. Частным случаем являются группы с двухмерной цикличностью.

Мультипликативная группа двухмерной конечной ассоциативной алгебры с операцией умножения, заданной в соответствии с табл. 2, представляет собой [12] циклическую группу, если структурный коэффициент λ является квадратичным невычетом в $GF(p)$, либо группу с двухмерной цикличностью, если λ является квадратичным вычетом в $GF(p)$. В первом случае порядок мультипликативной группы Ω описывается формулой

$$\Omega = p^2 - 1,$$

а во втором — формулой

$$\Omega = (p-1)^2.$$

В работах [11, 12] рассмотрены примеры коммутативных конечных групп с μ-мерной цикличностью для значений $\mu \geq 2$ и их применение для построения схем ЭЦП. В рамках данной работы рассмотрено применение коммутативной группы, обладающей двухмерным циклическим строением, в качестве скрытой группы. Предложенный способ построения схем ЭЦП на основе СЗДЛ может быть применен и в случае, когда в используемой в качестве алгебраического носителя КНАА содержатся группы с размерностью циклического строения $\mu \geq 3$.

Таблица 2

ТУБВ для задания двухмерной конечной алгебры над полем $GF(p)$ ($\lambda \neq 0$)

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$

При построении схем ЭЦП важным вопросом является задание групп, содержащих элементы, порядок которых равен простому числу достаточно большого размера. В этом случае в качестве характеристики p поля $GF(p)$ выбирают простое число $p = 2q + 1$, где q — 256-битное простое число. Тогда рассматриваемая группа с двухмерной цикличностью содержит подгруппу $\Gamma_{\langle \mathbf{G}, \mathbf{Q} \rangle}$ порядка q^2, порождаемую некоторым базисом $\langle \mathbf{G}, \mathbf{Q} \rangle$, содержащим два независимых вектора (в том смысле, что ни один из них не может быть представлен в виде натуральной степени другого), порядок каждого из которых равен простому числу q. Конечная группа $\Gamma_{\langle \mathbf{G}, \mathbf{Q} \rangle}$ содержит единичный вектор (1, 0) и $q^2 - 1$ различных векторов порядка q, которые образуют $q + 1$ циклических групп порядка q, попарно пересекающихся в единственном элементе — единичном векторе (1, 0).

Предлагаемый способ выполнения общего критерия постквантовой стойкости

Для выполнения общего критерия постквантовой стойкости в предлагаемом способе используем идею работы [10], состоящую в применении маскирующего умножения элементов базовой циклической группы (группы, в которой выполняется операция экспоненциирования) на перестановочный с ними элемент другой циклической группы, имеющей порядок, равный порядку базовой группы. При этом для существенного уменьшения размера подписи применяется новый способ формирования открытого ключа, который описывается следующим алгоритмом.

- Генерируем базис $\langle \mathbf{G}, \mathbf{Q} \rangle$ скрытой коммутативной группы $\Gamma_{\langle \mathbf{G}, \mathbf{Q} \rangle}$ с двухмерной цикличностью.
- Генерируем два случайных обратимых вектора $\mathbf{A}$ и $\mathbf{B}$, порядок каждого из которых равен $p^2 - 1$.
- Выбираем случайное неотрицательное целое число $x < q$ и вычисляем первый элемент открытого ключа в виде вектора $\mathbf{U} = \mathbf{A} \circ \mathbf{G}^x \circ \mathbf{B}^{-1}$. Умножение слева на $\mathbf{A}$ и справа на $\mathbf{B}^{-1}$ задает маскирующее отображение вектора $\mathbf{G}^x$, которое не является коммутативным с операцией экспоненцирования.
- Вычисляем второй элемент открытого ключа в виде вектора $\mathbf{Y} = \mathbf{B} \circ \mathbf{G} \circ \mathbf{B}^{-1}$. Умножение слева на $\mathbf{B}$ и справа на $\mathbf{B}^{-1}$ задает маскирующее отображение вектора $\mathbf{G}^x$, которое является коммутативным с операцией экспоненцирования.
- Вычисляем третий элемент открытого ключа в виде вектора $\mathbf{Z} = \mathbf{B} \circ \mathbf{Q} \circ \mathbf{A}^{-1}$. Умножение слева на $\mathbf{B}$ и справа на $\mathbf{A}^{-1}$ задает маскирующее отображение вектора $\mathbf{Q}$, которое не является коммутативным с операцией экспоненцирования.

Видно, что маскирующие операции связаны друг с другом и позволяют задать произведения двух или трех элементов открытого ключа, представимых в виде образов маскирующих отображений элементов скрытой группы, которые являются коммутативными с операцией возведения в степень. Это использовано для задания проверочного уравнения, обеспечивающего корректность работы схемы ЭЦП.

Генерацию базиса $\langle \mathbf{G}, \mathbf{Q} \rangle$ осуществляют по следующему алгоритму.

- Сгенерировать случайный вектор $\mathbf{R}$ и вычислить вектор $\mathbf{G} = \mathbf{R}^{(p^2-1)q^{-1}} \neq \mathbf{E}$, где $\mathbf{E}$ — единичный вектор восьмимерной КНАА, используемой в качестве алгебраического носителя.
- Используя целое число $\beta \in GF(p)$, имеющее значение порядка по модулю p, равное q, вычислить вектор $\mathbf{Q} = \beta\mathbf{G}$.

Таким образом, открытым ключом является тройка векторов $(\mathbf{U}, \mathbf{Y}, \mathbf{Z})$ и его размер равен 768 байтам. Все векторы и числа, использованные в процедуре формирования открытого ключа, являются секретными. Открытыми параметрами схемы ЭЦП служат элементы открытого ключа. Выполнимость общего критерия постквантовой стойкости обеспечивается тем, что при построении периодической функции на основе открытых параметров ее значения зависят от множителя $\mathbf{Q}$, наличие которого приводит к устранению периода, связанного со значением x. Без знания секретных векторов $\mathbf{A}$, $\mathbf{B}$, $\mathbf{G}$ и $\mathbf{Q}$ вычислительно сложно построить периодическую функцию, в которой устранено маскирующее влияние вектора $\mathbf{Q}$.

Например, рассмотрим периодическую функцию

$$F_1(i, j) = (\mathbf{U} \circ \mathbf{Y} \circ \mathbf{Z})^i (\mathbf{U} \circ \mathbf{Z})^j = \\ = \mathbf{A} \circ \mathbf{G}^{xi+i+j} \circ \mathbf{Q}^{i+j} \circ \mathbf{A}^{-1}.$$

Пусть длина периода этой функции равна (δ_i, δ_j). Тогда в силу независимости векторов $\mathbf{G}$ и $\mathbf{Q}$ имеем

$$\left\{ \begin{array}{c} x\delta_i + \delta_i + \delta_j \equiv 0 \bmod q \\ \delta_i + \delta_j \equiv 0 \bmod q \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} \delta_i \equiv 0 \bmod q \\ \delta_j \equiv 0 \bmod q \end{array} \right\},$$

т. е. функция $F_1(i, j)$ содержит только периоды, длина которых равна значениям (kq, tq) при целочисленных значениях k и t. Аналогично можно показать, что последнее утверждение верно и для следующей функции:

$$F_2(i, j) = (\mathbf{Z} \circ \mathbf{U})^i \mathbf{Y}^j = \mathbf{B} \circ \mathbf{Q}^i \circ \mathbf{G}^{xi+j} \circ \mathbf{B}^{-1}.$$

Вычисление и проверка подлинности подписи

Для вычисления ЭЦП к документу M выполняют следующий алгоритм.

- Сгенерировать два случайных целых числа $k < q$ и $t < q$ и вычислить вектор $\mathbf{V}$:

$$\mathbf{V} = \mathbf{A} \circ \mathbf{G}^k \circ \mathbf{Q}^t \circ \mathbf{A}^{-1}.$$

- Используя некоторую стойкую 256-битную хэш-функцию f_H, вычислить первый элемент подписи в виде числа $e = f_H(M, \mathbf{V})$.
- Вычислить второй элемент s цифровой подписи как решение квадратичного сравнения $es^2 - s + xt + t = k \bmod q$. Если последнее сравнение с неизвестным s не имеет решений, то перейти к шагу 1.
- Вычислить третий элемент d цифровой подписи по формуле $d = s^{-1}(t - s) \bmod q$.

В среднем для вычисления одной подписи, представляющей собой тройку 256-битных чисел (e, s, d), необходимо выполнить четыре операции экспоненцирования в КНАА, используемой в качестве алгебраического носителя. Длина подписи равна 96 байт.

Процедуру проверки подлинности подписи к документу M осуществляют по открытому ключу $(\mathbf{U}, \mathbf{Y}, \mathbf{Z})$ в соответствии со следующим алгоритмом.

- Вычислить вектор $\tilde{\mathbf{V}}$:

$$\tilde{\mathbf{V}} = \left(\mathbf{U} \circ \mathbf{Y}^{es} \circ \mathbf{Z} \circ (\mathbf{U} \circ \mathbf{Y} \circ \mathbf{Z})^d \right)^s.$$

- Вычислить значение $\tilde{e} = f_H(M, \tilde{\mathbf{V}})$.
- Если равенство $\tilde{e} = e$ выполнено, то подпись признается подлинной, иначе подпись отвергается.

Доказательство корректности разработанной схемы ЭЦП состоит в том, чтобы показать, что правильно вычисленная подпись (e, s, d) проходит процедуру проверки как подлинная, и выполняется следующим образом:

$$\tilde{\mathbf{V}} = \left(\mathbf{U} \circ \mathbf{Y}^{es} \circ \mathbf{Z} \circ (\mathbf{U} \circ \mathbf{Y} \circ \mathbf{Z})^d \right)^s = \\ = \left(\begin{array}{l} \mathbf{A} \circ \mathbf{G}^x \circ \mathbf{B}^{-1} \circ \mathbf{B} \circ \mathbf{G}^{es} \circ \mathbf{B}^{-1}\mathbf{B} \circ \mathbf{Q} \circ \mathbf{A}^{-1} \circ \\ \circ \left(\mathbf{A} \circ \mathbf{G}^x \circ \mathbf{B}^{-1} \circ \mathbf{B} \circ \mathbf{G} \circ \mathbf{B}^{-1} \circ \mathbf{B} \circ \mathbf{Q} \circ \mathbf{A}^{-1} \right)^d \end{array} \right)^s = \\ = \mathbf{A} \circ \mathbf{G}^{xs} \circ \mathbf{G}^{es^2} \circ \mathbf{Q}^s \circ \mathbf{G}^{xds} \circ \mathbf{G}^{ds} \circ \mathbf{Q}^{ds} \circ \mathbf{A}^{-1} = \\ = \mathbf{A} \circ \mathbf{G}^{es^2 + xs + ds(x+1)} \circ \mathbf{Q}^{s+ds} \circ \mathbf{A}^{-1} = \\ = \mathbf{A} \circ \mathbf{G}^{es^2 - s + tx + t} \circ \mathbf{Q}^{s+ds} \circ \mathbf{A}^{-1} = \\ = \mathbf{A} \circ \mathbf{G}^k \circ \mathbf{Q}^t \circ \mathbf{A}^{-1} = \mathbf{V} \Rightarrow \tilde{e} = e.$$

Сравнение с известными постквантовыми схемами подписи

В ходе конкурса НИСТ [2] для более детального рассмотрения в качестве кандидатов на постквантовый стандарт было отобрано девять схем ЭЦП [13]. С точки зрения компромисса между размерами открытого ключа и ЭЦП и производительностью алгоритмов формирования и проверки подлинности подписи предпочтительными представляются следующие кандидаты: Falcon [https://falcon-sign.info/], qTESLA [https://qtesla.org/], Rainbow [14] и Dilithium [https://pq-crystals.org/dilithium/index.shtml]. Представляет интерес сравнение разработанной постквантовой схемы ЭЦП с перечисленными кандидатами на постквантовый стандарт ЭЦП и со схемой ЭЦП [10], основанной на СЗДЛ и удовлетворяющей общему критерию постквантовой стойкости. Табл. 3 дает такое сравнение для версий сравниваемых схем ЭЦП, соответствующих 128-битной стойкости. Сравнение показывает, что схемы ЭЦП, основанные на СЗДЛ, обладают существенно меньшим суммарным размером подписи и открытого ключа и более высокой производительностью. При этом предложенная схема ЭЦП по сравнению со схемой подписи [10] обладает меньшей длиной подписи.

Таблица 3

Сравнение предложенной схемы ЭЦП с известными

Схема ЭЦП	Длина подписи, байт	Длина открытого ключа, байт	Скорость формирования ЭЦП, отн. ед.	Скорость верификации ЭЦП, отн. ед.
Falcon-512	657	897	5	3
qTESLA-p-I	2592	15000	3	6
Rainbow	64	150000	—	—
Dilithium	2044	1184	2	1
[10]	192	768	4	3
Предложенная	96	768	3	4

Существенный практический интерес представляет использование предложенного способа для построения постквантовых схем ЭЦП на четырехмерных КНАА, поскольку это позволит сократить размер открытого ключа в два раза, а производительность процедур генерации и проверки ЭЦП — более чем в два раза. Для этого следует указать в качестве алгебраического носителя алгебру, для которой можно доказать существование групп с двухмерной цикличностью и предложить способ задания таких групп в качестве скрытой группы. Предварительная проработка показывает потенциальную возможность реализации отмеченных двух требований для четырехмерных КНАА с глобальной двухсторонней единицей, однако детальное рассмотрение этого вопроса представляет собой тему самостоятельной работы.

Другим направлением развития предложенного способа является разработка на его основе схем ЭЦП с альтернативными проверочными уравнениями в целях повышения производительности процедуры проверки подписи.

Заключение

Предложен новый способ построения основанных на СЗДЛ схем ЭЦП, удовлетворяющих общему критерию постквантовой стойкости, который позволяет существенно сократить размер подписи по сравнению со способом, описанным в работе [10]. На основе данного способа разработана конкретная постквантовая схема ЭЦП, которая представляется более практичной по сравнению с известными кандидатами на постквантовый стандарт ЭЦП, предложенными в ходе конкурса НИСТ [2] по разработке постквантовых двухключевых криптосхем.

В целях дальнейшего сокращения размера открытого ключа и повышения производительности представляет интерес применение предложенного способа для разработки постквантовых схем ЭЦП, использующих четырехмерные и шестимерые КНАА в качестве алгебраического носителя, в том числе и КНАА, задаваемые по прореженным ТУБВ [15].

Литература

1. Post-Quantum Cryptography. 10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019, Proceedings // Lecture Notes in Computer Science series. Springer, 2019. V. 11505. —420 p.
2. Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. Available [Электронный ресурс]. Режим доступа: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf
3. *Молдовян Н. А., Абросимов И. К.* Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23—32.
4. *Moldovyan N. A., Moldovyan A. A.* Finite Non-commutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem // Вестник ЮУрГУ. Сер. "Математическое моделирование и программирование". 2019. Т. 12. № 1. С. 66—81.
5. *Молдовян А. А., Молдовян Д. Н.* Постквантовая схема ЭЦП на основе скрытой задачи дискретного логарифмирования в четырехмерной конечной алгебре // Вопросы защиты информации. 2019. № 2. С. 18—22.
6. *Moldovyan N. A., Moldovyan A. A.* Post-quantum signature algorithms based on the hidden discrete logarithm problem // Computer Science Journal of Moldova. 2018. V. 26. № 3(78). P. 301—313.
7. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM J. Computing. 1997. V. 26. P. 1484—1509.

8. *Ekert A., Jozsa R.* Quantum computation and Shor's factoring algorithm // Rev. Mod. Phys. 1996. V. 68. P. 733.
9. *Jozsa R.* Quantum algorithms and the fourier transform // Proc. Roy. Soc. London Ser A. 1998. V. 454. P. 323—337.
10. *Moldovyan D. N., Moldovyan A. A., Moldovyan N. A.* Digital signature scheme with doubled verification equation // Computer Science J. Moldova. 2020. V. 28. № 1(82). P. 80—103.
11. *Moldovyan N. A.* Fast signatures based on non-cyclic finite groups // Quasigroups and Related Systems. 2010. V. 18. № 1. P. 83—94.
12. *Moldovyan N. A., Moldovyanu P. A.* New primitives for digital signature algorithms // Quasigroups and Related Systems. 2009. V. 17. № 2. P. 271—282.
13. *Zimmer D.* NIST Round 2 and Post-Quantum Cryptography — The New Digital Signature Algorithms (2019) [Электронный ресурс]. Режим доступа: https://www.privateinternetaccess.com/blog/2019/02/nist-round-2-and-post-quantum-cryptography-the-new-digital-signature-algorithms
14. *Ding J., Schmidt D.* Rainbow, a New Multivariable Polynomial Signature Scheme // Lecture Notes in Computer Science. 2005. V. 3531. P. 164—175.
15. *Молдовян Д. Н., Молдовян А. А., Костина А. А.* Постквантовая схема цифровой подписи с двойным маскированием операции экспоненциирования // Вопросы защиты информации. 2020. № 2. С. 41—48.

An alternative method for designing signature schemes satisfying criterion of post-quantum security

A. A. Kostina, N. A. Moldovyan
St. Petersburg Federal Research Center of the RAS, St. Petersburg, Russia

In order to reduce the size of the public key and signature, a new method is proposed for constructing electronic digital signature schemes based on the hidden discrete logarithm problem, which satisfy the previously formulated post-quantum security criterion, which requires the elimination of periods associated with the value of the discrete logarithm in periodic functions specified by the public parameters of the cryptosystem. Based on the method, a digital signature scheme is developed, the basic primitive of which is an exponentiation operation in a hidden commutative group that has two-dimensional cyclicity. An eight-dimensional finite non-commutative associative algebra containing sufficiently large number of different groups with two-dimensional cyclicality is used as the algebraic carrier of the cryptosystem. The public key is three eight-dimensional vectors calculated depending on two vectors having prime order, which form the basis of the hidden commutative group. The digital signature is three 256-bit numbers.

Keywords: information protection, cryptography, digital signature, post-quantum cryptoscheme, discrete logarithm problem, finite associative algebra, non-commutative algebra.

Bibliography 15 references. *Received August 3, 2020*

УДК 003.26

Оценка сложности алгоритмов расчета параметров в схеме подписи на основе скрытой задачи дискретного логарифмирования

И. К. Абросимов
Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербург, Россия

Рассмотрены вычислительные алгоритмы над векторами конечных некоммутативных ассоциативных алгебр, выполнение которых требуется для работы схемы подписи, основанной на скрытой задаче дискретного логарифмирования. Выведены формулы для оценки сложности алгоритмов, используемых при работе схемы подписи, на их основе получены формулы для оценки сложности процедур формирования открытого ключа, формирования подписи и проверки подписи. Сложность алгоритмов выражена через количество операций умножения в поле, над которым задана алгебра.

Ключевые слова: постквантовая криптография, электронная подпись, конечные алгебры, сложность алгоритмов.

Электронная подпись является неотъемлемой частью электронного документооборота. Основой криптографической стойкости подписи является вычислительно трудная задача, которая делает невозможной подделку документа за обозримое время. Чаще всего в качестве таких задач используют задачи факторизации (ЗФ) и дискретного логарифмирования (ЗДЛ) [1]. Прогресс в области разработки вычислителей иного типа — квантовых компьютеров — и тот факт, что ЗФ и ЗДЛ могут быть решены на квантовом компьютере за полиномиальное время [2], требуют поиска новых вычислительно трудных задач, которые являются стойкими к атакам с помощью квантового компьютера. Среди предложенных в качестве кандидатов для нового криптографического стандарта схем подписи можно выделить схемы подписи CRYSTALS–DILITHIUM [3] и FALCON [4], остальные подписи, объявленные для участия в третьем раунде конкурса NIST [5], имеют слишком большие длины открытого и (или) секретного ключа либо подписи, из-за чего их практическая применимость сомнительна. В работе [6] предложена схема подписи на основе вычислительно трудной скрытой задачи дискретного логарифмирования (СЗДЛ), в качестве носителя которой используют конечные некоммутативные ассоциативные алгебры (КНАА). Сравнение производительности этой схемы подписи с производительностью схем CRYSTALS–DILITHIUM и FALCON можно осуществить посредством оценок сложности алгоритмов, используемых при процедурах формирования открытого ключа, формирования и проверки подписи. Для этого следует построить оценки данных процедур, зависящие от параметров схемы подписей, и сравнить их при тех значениях параметров схем сравниваемых подписей, которые обеспечивают одинаковую стойкость сравниваемых подписей к известным квантовым атакам.

Одной из особенностей схем, основанных на вычислительной трудности СЗДЛ над КНАА, является необходимость символьного вывода формул для параметров, используемых в схемах подписи [6, 7]. Для исключения такой необходимости требуется свести все вычисления к численным алгоритмам, причем независимо от того, какая именно КНАА была задана. После этого процедуры формирования открытого ключа, формирования подписи и проверки подписи будут представлять собой численные алгоритмы, сложность которых будет оцениваться.

При сравнении производительности схем подписей можно сформулировать следующие требования к функциям, описывающим оценки сложности алгоритма. Во-первых, необходимо построить оценку, более точную, чем асимптотическая оценка сложности процедур формирования открытого ключа, формирования подписи и проверки подписи, поскольку длины параметров, при которых сравнивают производительность схем, могут быть различными, что может влиять на скорость их ра-

Абросимов Иван Константинович, младший научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем.
E-mail: ivnabr@yandex.ru

Статья поступила в редакцию 18 августа 2020 г.

боты. Во-вторых, функции сложности должны выражать сложность алгоритма в виде количества одинаковых или по крайней мере похожих по сложности "атомарных" операций. В данной работе выведены формулы, которые явно (без нотации "о большое") связывают количество операций умножения в конечном поле с размерами входных данных. Под входными данными здесь понимается размерность КНАА и количество элементов конечного поля, над которым задана алгебра.

Описание схемы подписи, основанной на СЗДЛ в КНАА

В самом общем виде схемой подписи на основе двухключевой криптосистемы можно считать совокупность трех процедур: генерация открытого ключа, формирование подписи и проверка подписи. Поскольку один открытый ключ служит для подписания многих документов, можно утверждать, что производительность схемы подписи зависит в первую очередь от тех алгоритмов, которые используют для вычислений при формировании подписи и ее проверке.

Рассмотрим процедуры схемы подписи [6], основанной на СЗДЛ в КНАА. Процедура формирования открытого ключа, представляющего собой одно число (q) и три вектора ($\mathbf{y}$, $\mathbf{z}$, $\mathbf{l}$), заключается в выполнении следующих шагов:

- сгенерировать случайное простое число p длиной 512 бит и случайные числа x, w, t;
- сгенерировать необратимый вектор $\mathbf{g}$, длина порядка q которого равна 480 бит, обратимые векторы $\mathbf{v}$ и $\mathbf{u}$, попарно не коммутирующие друг с другом и с вектором $\mathbf{g}$, и правую локальную единицу $\mathbf{e}_{\mathbf{g}}$, ассоциированную с $\mathbf{g}$;
- вычислить $\mathbf{y}$, $\mathbf{z}$, $\mathbf{l}$ по формулам

$$\mathbf{y} = \mathbf{v}^{-w} \circ \mathbf{g}^{x} \circ \mathbf{v}^{w};$$

$$\mathbf{z} = \mathbf{u}^{-t} \circ \mathbf{g} \circ \mathbf{u}^{t};$$

$$\mathbf{l} = \mathbf{v}^{-w} \circ \mathbf{e}_{\mathbf{g}} \circ \mathbf{u}^{t}.$$

Следовательно, процедура формирования открытого ключа предполагает использование следующих специфических для КНАА операций:

- генерация случайного необратимого вектора заданного порядка;
- генерация случайного обратимого вектора;
- генерация локальной единицы, ассоциированной с данным вектором;
- возведение вектора в натуральную степень.

Формирование подписи состоит в вычислении разовых секретного и открытого ключей по формуле

$$\mathbf{r} = \mathbf{v}^{-w} \circ \mathbf{g}^{k} \circ \mathbf{u}^{t},$$

где $\mathbf{r}$ — разовый открытый ключ;
$1 < k < q-1$ — разовый секретный ключ.

Разовый открытый ключ используют для формирования первого элемента подписи:

$$e = F_H(\mathbf{m} \| \mathbf{r}),$$

где $\mathbf{m}$ — векторное представление подписываемого сообщения;
F_H — хеш–функция;
$\|$ — конкатенация векторов.

Разовый секретный ключ используют для формирования второго элемента подписи:

$$s = (k + ex) \bmod q.$$

Следовательно, процедура формирования подписи (e, s) предполагает использование возведения вектора в натуральную степень, операции вычисления хеш-функции и произведения по модулю.

Для проверки подписи используют следующее уравнение проверки:

$$\tilde{\mathbf{r}} = \mathbf{y}^{-e} \circ \mathbf{l} \circ \mathbf{z}^{s},$$

где (e, s) — проверяемая подпись документа.

Проверка состоит в вычислении $\tilde{e} = F_H(\mathbf{m} \| \mathbf{r})$ и последующем сравнении с первым элементом подписи. Если $\tilde{e} = e$, то подпись считают подлинной, в противном случае — поддельной.

Следовательно, процедура проверки подписи предполагает использование возведения вектора в натуральную степень, операции вычисления хеш-функции и произведения по модулю.

Таким образом, наиболее часто используемая операция при работе с подписью на основе СЗДЛ в КНАА — это возведение векторов в натуральную степень. Однако для полноты проводимого анализа далее будут рассмотрены все алгоритмы над векторами КНАА, которые используют для формирования секретного ключа в схеме подписи.

Используемая методика оценивания сложности вычислительных алгоритмов

Для оценивания сложности выполнения алгоритма используют символ "о большое", характеризующий рост сложности алгоритма при увеличе-

нии размера входных данных (асимптотическая оценка сложности алгоритма) [8]. При этом следует указывать операцию, относительно которой задается асимптотическая сложность. Однако для оценивания параметров каких-либо криптосистем эта характеристика может быть применена не всегда. Например, если аналогичные процедуры различных схем подписи имеют одинаковую асимптотическую сложность по одной и той же операции, то для сравнения этих схем необходимо использование других характеристик. Поэтому следует определять более точное значение функции временной сложности, чем описание ее в виде принадлежности некоторому классу функций через символ "о большое".

Оценивание сложности алгоритмов, используемых в схеме подписи на основе КНАА, будем производить следующим образом. Во-первых, выделим алгоритмы, сложность которых будем определять. Во-вторых, выберем "атомарные" операции, через выполнение которых будет выражена сложность рассматриваемых алгоритмов. И в-третьих, выполним подсчет функции временной сложности для каждой операции. При этом временную сложность будем подсчитывать в предположении, что операция умножения в КНАА задана конкретными значениями структурных констант алгебры. Тогда выполнение операций, необходимых для работы схемы подписи, сводится к уже известным численным алгоритмам. Рассмотрим эти операции подробнее.

Возведение вектора КНАА в натуральную степень сводится к умножению векторов, которое, в свою очередь, сводится к перемножению координат в соответствии со структурными константами, задающими умножение [9]. Следовательно, "атомарной" операцией для алгоритма возведения в степень будет перемножение чисел по модулю. Обращение вектора КНАА и генерация локальных единиц, ассоциированных с фиксированным вектором алгебры, требуют решения системы линейных уравнений [7, 9] над конечным полем. Наконец, генерация необратимого вектора требует несколько более сложной процедуры, если речь идет о полном исключении символьных вычислений.

Оценка сложности вычислительных алгоритмов, используемых в схеме подписи на основе КНАА

Свойство ассоциативности операции умножения в КНАА позволяет использовать быстрое возведение в степень [10] для вычисления натуральной степени вектора. Вычисление степени осуществляют следующим образом. Пусть необходимо вычислить k-ю степень вектора $\mathbf{v}$, тогда вычисления осуществляют согласно рекурсивной формуле

$$\mathbf{v}^k = \begin{cases} \left(\mathbf{v}^2\right)^{k/2}, & \text{если } k - \text{четное}; \\ \left(\mathbf{v}^2\right)^{(k-1)/2} \circ \mathbf{v}, & \text{если } k - \text{нечетное}. \end{cases}$$

Вычисления завершают при $k=1$. Согласно формуле для возведения в степень на каждом шаге показатель степени уменьшается вдвое, требуется выполнить возведение в квадрат, а в случае нечетности показателя степени — еще и умножение на основание степени. Следовательно, возведение в k-ю степень сводится к $\lfloor \log_2 k \rfloor$ возведениям в квадрат вектора и $1(k)-1$ умножениям векторов, где $1(k)$ — число единичных бит в двоичном представлении числа k. Таким образом, точная сложность операции возведения в степень составляет $\lfloor \log_2 k \rfloor + 1(k) - 1$ операций умножения векторов. Сверху эту величину можно оценить как $T_P(k) \le 2\lfloor \log_2 k \rfloor$, что дает асимптотическую сложность алгоритма $O(n)$ умножений, где n — двоичная длина показателя степени.

Для того чтобы свести операцию умножения векторов к операции умножения по модулю, необходимо рассмотреть операцию умножения векторов КНАА более подробно. Умножение двух векторов, $\mathbf{v} = (v_1, v_2, ..., v_d)$ и $\mathbf{w} = (w_1, w_2, ..., w_d)$, представляет собой попарное умножение координат с последующей заменой полученных произведений базисных векторов произведением структурной константы на некоторый базисный вектор:

$$\mathbf{v} \circ \mathbf{w} = \left(\sum_{i=1}^{d} v_i \mathbf{e}_i\right) \circ \left(\sum_{j=1}^{d} w_j \mathbf{e}_j\right) =$$

$$= \sum_{i,j} \left(v_i w_j (\mathbf{e}_i \circ \mathbf{e}_j)\right) = \sum_{i,j} \left(v_i w_j (T_{i,j} \circ \mathbf{e}_{k(i,j)})\right),$$

где $T_{i,j}$ — структурные константы;

$\mathbf{e}_i$, $\mathbf{e}_j$, $\mathbf{e}_{k(i,j)}$ — базисные векторы.

Дальнейшая группировка по базисным векторам требует использования только сложения по модулю. Таким образом, произведение двух векторов состоит в выполнении d^2 умножений по модулю при перемножении пар коэффициентов и

d^2 умножений получившихся произведений $v_i w_j$ на структурные коэффициенты (сложением по модулю для группировки слагаемых по одинаковым базисным векторам можно пренебречь), т. е. вычисление произведения двух векторов требует $2d^2$ операций умножения в поле, где d — размерность векторов алгебры.

Теорема 1. Сложность операции возведения вектора КНАА в степень k есть $T_P(k,d) = 2d^2\left(\lceil \log_2 k \rceil + 1(k) - 1\right)$ операций умножения в поле, где d — размерность векторов алгебры.

Генерация обратимого вектора КНАА может быть осуществлена следующим образом. Пусть задан обратимый вектор $\mathbf{v} = (v_1, v_2, ..., v_d)$, и требуется найти вектор $\mathbf{v}^{-1} = (x_1, x_2, ..., x_d)$, такой, что $\mathbf{v} \circ \mathbf{v}^{-1} = \mathbf{v}^{-1} \circ \mathbf{v} = \mathbf{e}_0$, где $\mathbf{e}_0$ — единица алгебры. Произведение $\mathbf{v} \circ \mathbf{v}^{-1}$ представляет собой линейную комбинацию по базисным векторам, каждый из которых в свою очередь представляет собой линейную комбинацию $f_i(x_1, x_2, ..., x_d)$ неизвестных координат вектора $\mathbf{v}^{-1}$. Поскольку векторы равны только тогда, когда равны коэффициенты при соответствующих базисных векторах, имеем систему d равенств вида

$$f_i(x_1, x_2, ..., x_d) = [\mathbf{e}_0]_i, \qquad (1)$$

где $[\mathbf{e}_0]_i$ — i-я координата вектора $\mathbf{e}_0$. Таким образом, уравнение $\mathbf{v} \circ \mathbf{v}^{-1} = \mathbf{e}_0$ равносильно системе линейных уравнений

$$\mathbf{V}\mathbf{X} = \mathbf{e}_0, \qquad (2)$$

где $\mathbf{V}$ — матрица коэффициентов линейных комбинаций из левых частей (1);

$\mathbf{X}$ — столбец координат вектора $\mathbf{v}^{-1}$.

Система (2) имеет единственное решение в силу обратимости $\mathbf{v}$. Таким образом, для нахождения вектора, обратного вектору $\mathbf{v}$, необходимо найти представление в виде (2), т. е. построить матрицу $\mathbf{V}$. Построение матрицы $\mathbf{V}$ требует выполнения d^2 умножений по модулю. Это следует из того, что при вычислении произведения $\mathbf{v} \circ \mathbf{v}^{-1}$ необходимо выполнить умножение d^2 пар базисных векторов и последующее умножение координат $\mathbf{v}$ на структурные константы.

Таким образом, полная оценка сложности алгоритма обращения вектора состоит в построении матрицы $\mathbf{V}$ и последующем решении системы (2).

Теорема 2. Сложность операции обращения вектора есть $T_{\mathrm{I}}(d) = d^2 + T_{\mathrm{SLS}}(d)$ операций умножения в поле, где $T_{\mathrm{SLS}}(d) \le 2d^3$ — сложность алгоритма решения системы линейных уравнений над конечным полем; d — размерность алгебры.

Алгоритм проверки обратимости вектора $\mathbf{v}$ можно построить следующим образом: строим матрицу $\mathbf{V}$ и вычисляем ее определитель; если определитель не равен 0, то вектор $\mathbf{v}$ обратим, в противном случае вектор $\mathbf{v}$ необратим. Поскольку определитель $\mathbf{V}$ считается над конечным полем, вероятность того, что случайный вектор имеет нулевой определитель, равна $1/q$, где q — число элементов конечного поля, над которым задана алгебра. Этот алгоритм нельзя использовать для проверки необратимости вектора, поскольку вероятность нахождения необратимого вектора равна $1/q \approx 1/2^{[\log_2 q]}$ при достаточно большом q (на практике q имеет длину не менее 512 бит).

Сложность алгоритма проверки обратимости вектора устанавливается теоремой.

Теорема 3. Для проверки вектора на обратимость требуется выполнить $T_{\mathrm{IT}}(d) = d^2 + T_{\det}(d)$ операций умножения в поле, где $T_{\det}(d) \le d^3$ — сложность алгоритма вычисления определителя матрицы $\mathbf{V}$.

Генерация локальной единицы, ассоциированной с данным вектором $\mathbf{v}$, состоит в случайном выборе элемента множества соответствующих (левосторонних или правосторонних) локальных единиц. Для определенности будем считать, что требуется выбрать случайную правую локальную единицу $\mathbf{e}_{\mathbf{v}}$, ассоциированную с вектором $\mathbf{v}$. Для формирования множества правых локальных единиц составим векторное уравнение:

$$\mathbf{v} \circ \mathbf{e}_{\mathbf{v}} = \mathbf{v},$$

где $\mathbf{e}_{\mathbf{v}} = (x_1, x_2, ..., x_d)$.

Выполнив преобразования, аналогичные алгоритму нахождения необратимого вектора, преобразуем это уравнение к системе линейных уравнений:

$$\mathbf{V}\mathbf{X} = \mathbf{v}, \qquad (3)$$

где $\mathbf{X} = (x_1, x_2, ..., x_d)$.

Если вектор $\mathbf{v}$ необратим, то $\det \mathbf{V} = 0$ и система (3) имеет более одного решения, поскольку равенство $\det \mathbf{V} = 0$ означает, что координаты вектора $\mathbf{v}$ связаны, причем таким же образом, как и элементы столбцов матрицы $\mathbf{V}$, из-за чего случай пустого множества решений становится невозможным. Следовательно, это решение будет иметь вид

$$\mathbf{X} = \mathbf{v}_0 + \sum_{i=1}^{d-\mathrm{rg}\,\mathbf{V}} \mathbf{v}_i t_i, \; t_i \in \mathrm{GF}(q),$$

где d — размерность алгебры, заданной над конечным полем $\mathrm{GF}(q)$.

Таким образом, множество

$$E_r(\mathbf{v}) = \left\{ \mathbf{v}_0 + \sum_{i=1}^{d-\mathrm{rg}\,\mathbf{V}} \mathbf{v}_i \, t_i, \; t_i \in \mathrm{GF}(q) \right\}$$

представляет собой множество правых локальных единиц, ассоциированных с вектором $\mathbf{v}$. Следовательно, нахождение случайной правой локальной единицы, ассоциированной с вектором $\mathbf{v}$, состоит из трех этапов: нахождения по вектору $\mathbf{v}$ матрицы $\mathbf{V}$ системы (3), решения системы (3) для построения множества $E_r(\mathbf{v})$ и выбора случайного элемента $E_r(\mathbf{v})$ путем выбора значений t_i, где $i \in \overline{1, d - \mathrm{rg}\,\mathbf{V}}$.

Выбор случайного элемента построенного множества $E_r(\mathbf{v})$ требует выполнения $d - \mathrm{rg}\,\mathbf{V}$ умножений вектора размерности d на скаляр. Умножение вектора на скаляр требует d операций умножения в поле.

Таким образом, сложность алгоритма генерации случайной локальной единицы устанавливается следующей теоремой.

Теорема 4. Генерация локальной единицы требует $T_{\mathrm{LU}}(d) = d^2 + T_{\mathrm{SLS}}(d) + d(d - \mathrm{rg}\,\mathbf{V})$ операций умножения в поле.

Генерация случайного необратимого вектора требует вычисления определителей уже не над элементами поля $\mathrm{GF}(q)$, над которым задается алгебра, а над многочленами с коэффициентами из поля $\mathrm{GF}(q)$. Находить необратимый вектор будем следующим образом. Зафиксируем все координаты будущего необратимого вектора $\mathbf{v}$, кроме одной (обозначим ее как x), выполним нахождение матрицы $\mathbf{V}$ аналогично ранее рассмотренным алгоритмам и вычислим ее определитель. Учитывая, что матрица $\mathbf{V}$ содержит либо константы, либо неизвестную координату x, получим многочлен $P(x)$, степень которого не превышает размерности алгебры d. Поскольку вектор необратим тогда и только тогда, когда $\det \mathbf{V} = 0$, для необратимости вектора $\mathbf{v}$ координата x должна быть корнем многочлена $P(x)$. Нахождение корней уравнения $P(x) = 0$ осуществим вероятностным алгоритмом Берлекэмпа–Рабина [11], вероятность успешного разложения многочлена на нетривиальные множители, на каждом раунде которого не менее $1/2$ [12] (всего требуется не более d успешных раундов), а асимптотическая сложность раунда равна $O(d^2 \log q)$ [13]. Поскольку для нахождения необратимого вектора достаточно найти один корень уравнения $P(x) = 0$, справедлива следующая теорема.

Теорема 5. Генерация необратимого вектора имеет сложность $T_{\mathrm{NI}}(d,q) = d^2 + 4T_{\det}(d) + Cd^2[\log d][\log q]$, где $C > 0$ — некоторая константа.

Оценка сложности процедур, используемых в схеме подписи на основе КНАА

Сложность процедур формирования открытого ключа, формирования и проверки подписи устанавливают теоремы 6—8. В этих теоремах рассмотрена сложность операций с элементами КНАА и не учтены сложности процедур генерации случайных чисел и вычисления хеш-функции.

Теорема 6. Сложность процедуры формирования открытого ключа есть $T_{\mathrm{PKG}}(d,q) \le (Cd^2 \log d + 12d^2)\log q + 13d^3 + 31d^2$ операций умножения в поле, где q — число элементов поля, над которым задана алгебра. Здесь учтено, что порядок необратимого вектора **g** близок по размеру к числу элементов поля (например, 512-битное поле и 480-битный порядок необратимого вектора **g**).

Доказательство. Из описания процедуры формирования открытого ключа имеем

$$T_{\mathrm{PKG}}(d,q) = T_{\mathrm{NI}}(d,q) + 2T_{\mathrm{IT}}(d) + 12d^2 + T_{\mathrm{LU}}(d) + 3T_{\mathrm{P}}(q,d) + 2T_{\mathrm{I}}(d) + 12d^2.$$

Учитывая, что

$$T_{\mathrm{NI}}(d,q) = d^2 + 4T_{\det}(d) + Cd^2 \log d \log q \le Cd^2 \log d \log q + 4d^3 + d^2;$$

$$T_{\mathrm{IT}}(d) = d^2 + T_{\det}(d) \le d^3 + d^2;$$

$$T_{\mathrm{LU}}(d) = d^2 + T_{\mathrm{SLS}}(d) + d(d - \operatorname{rg}\mathbf{V}) \le 3d^3 + 2d^2;$$

$$T_{\mathrm{P}}(q,d) \le 2d^2 \cdot 2\lceil \log_2 q \rceil = 4d^2 \lceil \log_2 q \rceil;$$

$$T_{\mathrm{I}}(d) = d^2 + T_{\mathrm{SLS}}(d) \le 2d^3 + d^2,$$

имеем $T_{\mathrm{PKG}}(d,q) = (Cd^2 \log d + 12d^2)\log q + 13d^3 + 31d^2$, что и требовалось доказать. Следовательно, асимптотическая сложность процедуры формирования открытого ключа есть $O\left(d^2 \log d \log q + d^3\right)$ операций умножения в поле.

Теорема 7. Сложность процедуры формирования подписи есть $T_{\mathrm{SG}}(d,q) \le \left(4\lceil \log_2 q \rceil + 5\right) d^2$ операций умножения в поле.

Доказательство. Из описания процедуры формирования подписи имеем

$$T_{\mathrm{SG}}(d,q) = T_{\mathrm{P}}(q,d) + 4d^2 + d^2 \le$$

$$\le 2d^2 \cdot 2\lceil \log_2 q \rceil + 5d^2 = (4\lceil \log_2 q \rceil + 5)d^2,$$

что и требовалось доказать.

Теорема 8. Сложность процедуры проверки подписи есть $T_{\mathrm{SV}}(d,q) \le 4d^2 \lceil \log_2 q \rceil + 2d^3 + 5d^2$ операций умножения в поле.

Доказательство. Из описания процедуры проверки подписи имеем

$$T_{\mathrm{SV}}(d,q) = T_{\mathrm{I}}(d) + 2T_{\mathrm{P}}(q,d) +$$

$$+ 4d^2 \le 4d^2 \lceil \log_2 q \rceil + 2d^3 + 5d^2,$$

что и требовалось доказать. Учитывая, что вектор, обратный к вектору $\mathbf{y}$, можно вычислить только один раз для одного и того же открытого ключа, получим уменьшение сложности:

$$T_{\mathrm{SV}}^{'}(d,q) \le \left(\lceil \log_2 q \rceil + 1\right) 4d^2.$$

Таким образом, асимптотические сложности процедур формирования и проверки подписи одинаковы и составляют $O\left(d^2 \lceil \log_2 q \rceil\right)$ операций умножения в поле.

Заключение

Рассмотрены основные вычислительные алгоритмы, необходимые для выполнения вычислений в схеме подписи на основе СЗДЛ в КНАА. Получены оценки временной сложности для процедур формирования открытого ключа, формирования подписи и проверки подписи, выраженные в количестве операций умножения в поле. Представляют интерес уточнение константы C в формуле сложности процедуры генерации необратимого вектора и сравнение полной сложности процедур, используемых в схеме подписи на основе СЗДЛ, с соответствующими процедурами других постквантовых схем подписи.

Литература

1. *Menezes A. J., Van Oorschot P. C., Vanstone S. A.* Handbook of Applied Cryptography. — Boca Raton, FL: CRC Press, 1997.
2. *Shor P. W.* Polynomial–time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM J. Computing. 1997. V. 26. P. 1484—1509.
3. *Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehle D.* CRYSTALS–Dilithium: a Lattice–based Digital Signature Scheme // IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018. № 1. P. 238—268.
4. *Pornin T.* New Efficient, Constant–Time Implementations of Falcon [Электронный ресурс]. URL: htts://falcon–sign.info/falcon–impl–20190918.pdf (дата обращения: 14.08.2020).
5. PQC Standardization Process: Third Round Candidate Announcement [Электронный ресурс]. URL: http://csrc.nist.gov/News/2020/pqc–third–round–candidate–announcement (дата обращения: 14.08.2020).
6. *Молдовян Н. А., Абросимов И. К.* Схема постквантовой электронной цифровой подписи на основе усиленной формы скрытой задачи дискретного логарифмирования // Вестник Санкт-Петербургского ун-та. Прикладная математика. Информатика. Процессы управления. 2019. Т. 15. Вып. 2. С. 212—220.
7. *Молдовян Н. А., Абросимов И. К.* Постквантовая схема ЭЦП на основе скрытой задачи дискретного логарифмирования в четырехмерной конечной алгебре // Вопросы защиты информации. 2019. № 2. С. 18—22.
8. *Абрамов С. А.* Лекции о сложности алгоритмов. — М.: МЦНМО, 2009.
9. *Молдовян Н. А., Абросимов И. К., Ковалева И. В.* Постквантовый протокол бесключевого шифрования // Вопросы защиты информации. 2017. № 3. С. 3—13.
10. *Габидулин Э. М., Кшевецкий А. С., Колыбельников А. И.* Защита информации: учеб. пособие. — М.: МФТИ, 2011.
11. *Berlekamp E. R.* Factoring polynomials over large finite fields // Mathematics of Computation. 1970. V. 24(111). P. 730—732.
12. *Rabin M.* Probabilistic Algorithms in Finite Fields // SIAM J. Computing. 1980. V. 9(2). P. 273—280.
13. *Ben-Or M.* Probabilistic algorithms in finite fields: 22nd Annual Symposium on Foundations of Computer Science (sfcs 1981). 1981. P. 394—398.

Complexity evaluation of the parameters calculation algorithms in the signature scheme based on the hidden discrete logarithm problem

I. K. Abrosimov
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg, Russia

We consider computational algorithms over vectors of finite non-commutative associative algebras, the execution of which is required for the operation of the signature scheme based on the hidden problem of discrete logarithm. Formulas for evaluating algorithms complexity that used in the operation of the signature scheme are derived and on their basis, formulas for evaluating the procedures complexity for generating a public key, generating a signature and verifying a signature are obtained. The complexity of algorithms in multiplication operations of the field over which is given the algebra is measured.

Keywords: post-quantum cryptography, electronic signature, finite non-commutative associative algebras, algorithm complexity.

Bibliography 13 references. *Received August 18, 2020*

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004.056

Принципы разработки и реализации передовой образовательной программы высшего образования по направлению "информационная безопасность"

Т. М. Каннер
ЗАО "ОКБ САПР", Москва, Россия
Московский физико-технический институт (национальный исследовательский университет), г. Долгопрудный, Московская обл., Россия

Проанализированы недостатки существующих основных образовательных программ высшего образования (ООП ВО). Далее приведены принципы разработки и реализации передовых ООП ВО по приоритетным направлениям подготовки высшего образования с учетом запросов партнеров реального сектора экономики и мировых научно-технологических трендов. Рассмотрено применение данных принципов при разработке и реализации передовой ООП ВО по направлению "информационная безопасность".

Ключевые слова: информационная безопасность, передовая образовательная программа высшего образования, компетентностно-ориентированный подход, онлайн-курс, тиражирование образовательной программы.

В высших учебных заведениях существует большое количество различных основных образовательных программ высшего образования различных уровней подготовки: бакалавриат, специалитет, магистратура, в том числе и по направлению "информационная безопасность". Однако часть этих программ направлена в основном на теоретическое освоение материала. При этом практическое применение теоретических знаний отрабатывают на используемых много лет практических и лабораторных занятиях, в некоторых случаях не соответствующих современному уровню развития области защиты информации и потребностям работодателей в определенных умениях и навыках требуемых специалистов. Как правило, это связано с отсутствием соответствующих знаний у преподавательского состава и отсутствием взаимодействия образовательных организаций с организациями реального сектора экономики. В результате выпускники обладают компетенциями, не соответствующими ушедшей далеко вперед профессиональной деятельности и после обучения остаются невостребованными на рынке труда. При этом потребность организаций реального сектора экономики в специалистах с соответствующими компетенциями остается актуальной. Таким образом, возникает противоречие: существует потребность в специалистах, имеющих необходимые знания, умения и навыки, которые отсутствуют у выпускников, обученных по действующим программам высшего образования. Особенно заметно это противоречие проявляется в быстро развивающейся области защиты информации.

Помимо этого процесс обучения по существующим программам строится на привычных технологиях: обучение проводят очно, без использования таких современных технологий, как обучение на онлайн-курсах или с помощью систем дистанционного обучения. При этом студенты зачастую не имеют представления о наличии таких технологических возможностей, а преподаватели — опыта использования этих возможностей в процессе обучения.

Далее приведены принципы разработки и реализации передовых ООП ВО по приоритетным направлениям подготовки высшего образования с учетом запросов партнеров реального сектора экономики и мировых научно-технологических трендов, позволяющие устранить перечисленные недостатки. Рассмотрено применение данных принципов при разработке и реализации передовой ООП ВО по приоритетному направлению "информационная безопасность".

Каннер Татьяна Михайловна, руководитель учебного центра ЗАО «ОКБ САПР», ведущий инженер лаборатории "Прикладные исследования МФТИ—Сбербанк".
E-mail: tatianash@okbsapr.ru

Статья поступила в редакцию 9 сентября 2020 г.

Формирование принципов разработки и реализации передовых ООП ВО

Формирование принципов разработки и реализации передовых ООП ВО по приоритетным направлениям подготовки основано на стратегиях развития системы высшего образования Российской Федерации с учетом задач, сформированных национальным проектом "Образование", в рамках достижения результата федерального проекта "Молодые профессионалы (Повышение конкурентоспособности профессионального образования)" [1].

Одним из важных положений данного проекта является необходимость разработки образовательными организациями высшего образования совместно с партнерами реального сектора экономики адаптивных, практико-ориентированных, гибких образовательных программ высшего образования, которые обеспечат получение студентами профессиональных компетенций, отвечающих актуальным требованиям рынка труда, в том числе в области цифровой экономики, предпринимательства, командной и проектной работы, здоровьесбережения применительно к их будущим областям профессиональной деятельности. Также важными положениями проекта являются необходимость постоянного обновления профессиональных знаний и компетенций научно-педагогических работников на основе актуальных достижений науки и технологий, современных профессиональных требований, перспективных задач отрасли и необходимость участия преподавателей в исследованиях и разработках по вопросам, относящимся к предмету преподавания с привлечением к этим исследованиям обучающихся. Помимо этого обучающиеся по ООП ВО должны осваивать отдельные курсы, дисциплины (модули), в том числе в формате онлайн-курсов, с использованием ресурсов иных организаций, осуществляющих образовательную деятельность (университетов, обеспечивающих соответствие качества подготовки обучающихся мировому уровню, и т. д.).

Таким образом, изучив и суммировав все положения федерального проекта, можно сделать вывод, что актуальным направлением развития системы высшего образования Российской Федерации являются повышение качества ООП ВО и создание мотивационных факторов для научно-педагогических работников к разработке новых передовых междисциплинарных экспортно-ориентированных образовательных программ высшего образования и их отдельных дисциплин по приоритетным специальностям и направлениям подготовки высшего образования. Такие специальности и направления определены в приказе Министерства образования и науки РФ [2]. К ним в том числе относится укрупненная группа направлений подготовки 10.00.00 Информационная безопасность.

Для решения поставленной федеральным проектом задачи по повышению конкурентоспособности профессионального образования проведено изучение опыта ведущих мировых образовательных организаций. В рамках данного вопроса изучены существующие решения по повышению качества реализуемых образовательных программ высшего образования в РФ и за рубежом: проведен обзор образовательных программ, их особенностей и форматов реализации, решений по повышению эффективности привлечения научно-педагогических работников к разработке новых программ высшего образования и их отдельных дисциплин; изучены основные модели достижения данной цели образовательными организациями.

На основании положений рассмотренного федерального проекта и проведенного исследования мирового опыта сформулированы принципы разработки и реализации передовых ООП ВО, в соответствии с которыми передовая образовательная программа высшего образования должна:

- быть разработана и реализована совместно с образовательной организацией, входящей в топ-200 предметных глобальных рейтингов, в целях перенятия опыта ее высококвалифицированных научно-педагогических работников;
- быть разработана, реализована и тиражирована научно-педагогическими работниками и работниками административно-управленческого состава, прошедшими повышение квалификации и стажировку в организации, входящей в топ-200 предметных глобальных рейтингов;
- быть образовательной программой высшего образования, иметь междисциплинарный характер, соответствовать действующему федеральному государственному образовательному стандарту (ФГОС ВО), в том числе обеспечивать компетентностно-ориентированный подход;
- предусматривать формирование компетенций в области цифровой экономики, предпринимательства, командной и проектной работы;
- учитывать результаты передовых научных исследований и разработок;
- быть разработана и реализована совместно с работниками организаций из реального сектора экономики, быть востребованной в реальном секторе экономики и включать возможности прохождения практики, предусмотренной передовой образовательной программой, в организациях реального сектора экономики, а также быть реализуемой в условиях предварительно заключенных

договоров с такими организациями о намерениях по прохождению стажировок и трудоустройству студентов, завершивших обучение по передовой образовательной программе;

- включать дисциплину (модуль), реализуемую с использованием современных технологий образования, — онлайн-курса, размещенного на одной из 39 российских образовательных платформ, интегрированных с государственной информационной системой "Современная цифровая образовательная среда";
- включать экспортно-ориентированную дисциплину (модуль), реализуемую с использованием современных технологий образования, — массового открытого онлайн-курса (МООК) на иностранном языке, размещенного на одной из международных образовательных онлайн-платформ;
- обеспечивать возможность ее тиражирования в российских образовательных организациях высшего образования, в том числе с использованием механизмов сетевой формы реализации образовательных программ, в целях передачи (распространения) образовательного контента.

Реализация принципов в передовой ООП ВО по направлению "информационная безопасность"

Перечисленные принципы положены в основу разработанной ФГАОУ ВО "Уральским федеральным университетом им. первого Президента России Б. Н. Ельцина" (УрФУ) совместно с ФГАОУ ВО "Московским физико-техническим институтом (национальный исследовательский университет)" (МФТИ) и планируемой в ближайшее время к реализации передовой образовательной программы высшего образования "Защита информации в информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС) и значимых объектах критической информационной инфраструктуры (КИИ)" по направлению подготовки 10.04.01 Информационная безопасность (уровень — магистратуры).

МФТИ входит в топ-200 предметных глобальных рейтингов. При разработке ООП ВО использован опыт его высококвалифицированных научно-педагогических работников. Помимо этого до начала разработки ООП ВО в целях обновления профессиональных знаний и компетенций научно-педагогических работников УрФУ проведено повышение их квалификации в МФТИ по программе "Защита информации в ИСПДн, ГИС и значимых объектах КИИ".

Программа разработана на основе требований ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры), утвержденного приказом Министерства образования и науки РФ [3], в том числе с учетом обеспечения компетентностно-ориентированного подхода.

Целью реализации данной программы являются совершенствование и (или) получение новых компетенций, необходимых для осуществления профессиональной деятельности по информационной безопасности применительно к информационным системам персональных данных, государственным информационным системам и значимым объектам критической информационной инфраструктуры.

В учебном плане ООП ВО представлены дисциплины базовой и вариативной части. По каждой дисциплине и практикам определены компетенции выпускника, формируемые в процессе освоения образовательной программы: общекультурные, общепрофессиональные и профессиональные. Общая совокупность компетенций расширена с учетом профиля подготовки за счет дополнительных профессиональных компетенций в области цифровой экономики, предпринимательства, командной и проектной работы. Тем самым реализован компетентностно-ориентированный подход к формированию основной образовательной программы.

В программе рассмотрены актуальные в Российской Федерации вопросы, разбираемые в дисциплинах "Правовые аспекты информационной безопасности ИСПДн, ГИС и значимых объектов КИИ", "Методы и средства защиты информации в ИСПДн, ГИС и значимых объектов КИИ", "Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектов КИИ", "Меры и средства защиты информации от несанкционированного доступа (НСД) в ИСПДн, ГИС и значимых объектах КИИ", "Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ" и т. д. В результате прохождения программы студенты приобретают знания, умения и навыки в области обеспечения безопасности ИСПДн, ГИС и значимых объектов КИИ. В том числе студенты получают навыки установки, настройки и администрирования различных современных широко применяемых в различных организациях страны программно-аппаратных комплексов защиты информации одного из ведущих российских производителей — компании "ОКБ САПР".

В процессе разработки программы МФТИ проведен еще один курс повышения квалификации научно-педагогических работников УрФУ по программе "Защита персональных данных", соответ-

ствующей профилю ООП ВО. Данное повышение квалификации проводилось в целях получения сотрудниками УрФУ компетенций, необходимых в том числе для высокопрофессионального преподавания дисциплин, рассматривающих внедренные в процесс обучения программно-аппаратные комплексы защиты информации.

Также важное место в ООП ВО занимают модули, связанные с подготовкой специалистов по линии государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), такие, как "Организация и функционирование центров мониторинга Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак" и "Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры". Формируемые при изучении дисциплин этих модулей компетенции, знания, умения и навыки позволяют подготовить специалистов, необходимых для функционирования ведомственных и корпоративных центров ГосСОПКА на информационные ресурсы Российской Федерации. Специалисты такой направленности являются особенно востребованными соответствующими организациями после вступления в действие ФЗ-187 о безопасности критической информационной инфраструктуры [4]. При проведении анализа актуальных потребностей рынка выявлена заинтересованность ряда организаций региона расположения УрФУ в таких специалистах, т. е. программа является востребованной в реальном секторе экономики.

Помимо этого определен социальный партнер программы из реального сектора экономики — организация-работодатель, основная деятельность которой связана с защитой информации. Таким партнером стало ООО "Уральский центр систем безопасности" (УЦСБ). Экспертная группа партнера согласовала характеристики профессиональной деятельности выпускников по разработанной образовательной программе, в том числе область, объекты, виды профессиональной деятельности и профессиональные компетенции, тем самым подтвердив заинтересованность в ее выпускниках. Взаимодействие с УЦСБ включает возможность прохождения студентами практики, предусмотренной передовой образовательной программой. Также имеются предварительно заключенные договора о намерениях по прохождению стажировок и трудоустройству студентов, завершивших обучение по передовой образовательной программе.

Программа предусматривает использование таких современных технологий, как онлайн-обучение. В связи с этим одну из ее дисциплин — "Меры и средства защиты информации от несанкционированного доступа" — реализуют с использованием онлан-курса, разработанного МФТИ и размещенного на российской образовательной платформе "Национальная платформа открытого образования"*. Также программа включает экспортно-ориентированную дисциплину "Основы научного исследования", реализуемую с использованием разработанного МФТИ массового открытого онлайн-курса (МООК) на иностранном языке, размещенного на международной образовательной онлайн-платформе Coursera, с возможностью прохождения данного МООК иностранными слушателями.

При этом сотрудники УрФУ прошли повышение квалификации по программе "Разработка заданий в МООК". Данное повышение квалификации позволит осуществлять дальнейшую содержательную поддержку онлайн-курсов и их внедрение в рамках реализации ООП ВО, а также выполнять их тиражирование в другие образовательные организации.

В результате освоения дисциплин при помощи онлайн-курсов студенты освоят не только предусматриваемые компетенции, но и дополнительную компетенцию, в соответствии с которой они смогут владеть навыками использования современных технологий для самостоятельного приобретения знаний.

Рабочие программы модулей, дисциплин и фонды оценочных средств составлены с учетом обеспечения возможности тиражирования разработанной образовательной программы в российских организациях высшего образования, в том числе с использованием механизмов сетевой формы реализации образовательных программ. Такая форма является одной из наиболее востребованных и эффективных мер повышения конкурентоспособности образовательных организаций. Предполагается поэтапное тиражирование дисциплин ООП ВО в нескольких российских образовательных организациях высшего образования.

Заключение

Приведены принципы разработки и реализации передовой ООП ВО по приоритетным направле-

* https://openedu.ru/ — онлайн-платформа, интегрированная с государственной информационной системой "Современная цифровая образовательная среда".

ниям подготовки высшего образования с учетом запросов партнеров реального сектора экономики и мировых научно-технологических трендов. Рассмотрена реализация данных принципов в передовой основной образовательной программе высшего образования по приоритетному направлению подготовки "информационная безопасность". Дальнейшее применение описанного подхода к большинству реализуемых в образовательных организациях программ позволит готовить высококвалифицированных востребованных на рынке труда специалистов, в том числе в области защиты информации. Это, в свою очередь, должно постепенно вывести российское высшее образование на новый конкурентоспособный уровень.

ЛИТЕРАТУРА

1. Федеральный проект "Молодые профессионалы (Повышение конкурентоспособности профессионального образования)" [Электронный ресурс]. Режим доступа: https://futurerussia.gov.ru/molodye-professionaly-povysenie-konkurentosposobnosti-professionalnogo-obrazovania (дата обращения: 03.09.2020).

2. Приказ Министерства образования и науки Российской Федерации от 12.09.2013 № 1061 "Об утверждении перечней специальностей и направлений подготовки высшего образования".

3. Приказ Министерства образования и науки Российской Федерации от 01.12.2016 № 1513 "Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры)".

4. Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

Principles of development and implementation of the advanced educational program for the higher education in the "Information security" area

T. M. Kanner
JSC "OKB SAPR", Moscow, Russia
Moscow Institute of Physics and Technology (National Research University), Dolgoprudny, Moscow region, Russia

The article discusses the shortcomings of the existing basic educational programs for the higher education. The article describes the principles of development and implementation of advanced educational programs for the higher education in priority areas of training, taking into account the requests of partners in the real sector of the economy, world scientific and technological trends. The article considers the application of these principles in the development and implementation of the advanced educational programs for the higher education in the Information security area.

Keywords: information security, advanced educational program for the higher education, competence-based approach, online course, replication of the educational program.

Bibliography — 4 references. *Received September 9, 2020*

УДК 004.5

Синтез целеустремленных систем в условиях информационно-сложных ситуаций

В. А. Доровской, д-р техн. наук; *Б. П. Новак*; *А. В. Дегтярев*;
А. С. Соболев; *П. А. Ерофеев*
Керченский государственный морской технологический университет, г. Керчь, Россия

В результате исследования организационных объектов идентифицирован класс целенаправленных (или целеустремленных) систем с учетом базовых целей, которые задают извне (обычно это имеет место в закрытых системах), и систем, в которых цели формируют внутри системы (что характерно для открытых, самоорганизующихся систем). Проведены интроспективный анализ и синтез целеустремленных систем в условиях информационно-сложной ситуации с явно выраженными целевыми устремлениями по достижению цели. Исследования класса систем управления движущимися морскими объектами (судами и кораблями) в информационно-сложных ситуациях и деятельности таких систем, нацеленных на результат, который может быть достигнут при наличии обратной связи.

Ключевые слова: интроспективный анализ, интроспективный синтез, целеустремленные системы, информационно-сложная ситуация, полиустремленные системы.

Актуальность проблемы

Не всегда при изучении систем можно применять понятие "цель". Однако при изучении организационных объектов важно выделять класс целенаправленных (или целеустремленных) систем. В этом классе, в свою очередь, можно выделить системы, в которых цели задают извне (обычно это имеет место в закрытых системах), и системы, в которых цели формируют внутри системы (что характерно для открытых, самоорганизующихся систем). Целеустремленные системы являются системами с явно выраженными целевыми устремлениями по достижению цели. Как правило, это системы управления движущимися морскими объектами (судами и кораблями) в условиях информационно-сложных ситуаций. Деятельность таких систем нацелена на результат, который может быть достигнут при наличии обратной связи. Представлены интроспективный анализ и синтез таких систем.

Цель исследований — проведение интроспективного анализа и синтеза целеустремленных систем в условиях информационно-сложной ситуации.

Результаты исследований

Совместная активность множества целеустремленных динамических объектов $\mathrm{A} = \{A_0, A_1, \ldots, A_n\}$ на общем пространстве C приводит к их взаимодействию, в результате чего формируется полицелеустремленная система (ПЦС) Ξ на основе локальной близости динамических объектов, порожденной заданной метрикой ξ_C в пределах определенной области $C' \in C$.

На множестве динамических объектов $\mathrm{A} = \{A_0, A_1, A_2, A_3\}$ задают отношение χ, определяющее подмножество взаимодействующих динамических объектов A^C. Не все динамические объекты в конкретный момент времени в пределах $C' \in C$ являются взаимодействующими: $\mathrm{A} = \{A_0, A_1, A_2, A_3\}$, в то время как $\mathrm{A}^C = \{A_0, A_1, A_2\}$, т. е.

$$\{A_i,\ A_j\} \in \mathrm{A}^C \leftrightarrow \chi(A_i, A_j)\ \forall\ A_i,\ A_j \in \mathrm{A}. \qquad (1)$$

Поэтому вводят метрики $\xi_1, \ldots, \xi_k$, с помощью которых определяют степень взаимодействия динамических объектов друг с другом, что позволяет осуществить их классификацию.

Доровской Владимир Алексеевич, профессор кафедры "Электрооборудование судов и автоматизация производства".
E-mail: dora1943@mail.ru
Новак Богдан Петрович, аспирант кафедры "Электрооборудование судов и автоматизация производства".
E-mail: bogdan.dsl94@gmail.com
Дегтярев Андрей Владимирович, аспирант кафедры "Электрооборудование судов и автоматизация производства".
E-mail: esiap@mail.ru
Соболев Александр Сергеевич, инженер кафедры "Электрооборудование судов и автоматизация производства".
E-mail: sobolev.alexandr1496@gmail.com
Ерофеев Павел Андреевич, аспирант кафедры "Электрооборудование судов и автоматизация производства".
E-mail: pavel.erofeev.95@mail.ru

Статья поступила в редакцию 15 сентября 2020 г.

Формирование ПЦС Ξ может происходить двумя способами в зависимости от установленного отношения локальной близости:

- к конкретному динамическому объекту A_0, который в данном случае называют оперирующим, а область взаимодействия — динамической, т. к. C' перемещается вместе с A_0 в соответствии с $\beta(A_0)$;
- к конкретной области пространства $C' \in C$, которая в таком случае является статической в C.

В обоих случаях состав множества взаимодействующих динамических объектов A^C изменяется во времени: одни из них входят в область взаимодействия, другие, наоборот, ее покидают, что определяется их траекториями активности $\beta(A_0)$. Известно, что ПЦС относятся к классу сложных динамических систем и, кроме того, принадлежат к классу открытых систем, поскольку состав и структура ПЦС, ее взаимодействие с внешней средой эволюционируют во времени. Так как лицо, принимающее решение (ЛПР) в Ξ, реализует целенаправленное управление динамического объекта, планируя траекторию активности в пространстве взаимодействия и компенсируя возникающие возмущения ее изменением, полицелеустремленные системы необходимо рассматривать как класс открытых сложных динамических систем с целенаправленным поведением динамических объектов.

Всякий динамический объект $A_i \in \mathrm{A}^\chi$, взаимодействуя с динамическим объектом A_0, представляет собой ситуационное возмущение ω_i для A_0: активность динамического объекта A_i представляет собой динамическое ограничение $R_D^{\omega_i} \in Z_{A_0}$ и возмущает его траекторию активности $\beta(A_0)$.

ЛПР динамического объекта A_0 должно компенсировать ω_i таким же образом, как и внешние динамические возмущения w_j, изменяя траекторию активности $\beta(A_0)$ подачей вектора УВ $\bar{U}(\omega_i)$ на ИУ $\varphi_j \in \Im(A_0)$. Однако выполнение компенсации $M(\omega_i)$ является существенно более сложным вследствие корреляции решений ЛПР взаимодействующих динамических объектов A_i, а также наличия субъективных установок $Z_i = \langle G_i, Q_i, R_i \rangle$ (их цели G_i, критерии Q_i и ограничения R_i в общем случае неизвестны ЛПР других динамических объектов).

Значительный негативный вклад вносит и рефлексивный аспект принятия решений ЛПР [1—5] в условиях совместной активности. Компенсируя ситуационное возмущение ω_{i0} от A_i, ЛПР динамического объекта A_0 вносит возмущение ω_{0j} для A_j. В свою очередь ЛПР динамического объекта A_j, компенсируя ω_{0j}, вносит возмущение ω_{ij} для A_i, ЛПР которого, компенсируя ω_{ij}, пересматривает параметры своей активности и тем самым вектор возмущения ω_{i0}. Это вынуждает ЛПР динамического объекта A_0 трансформировать $\bar{U}(\omega_{i0})$, модифицируя ω_{0j}. Процесс многократно повторяется: взаимодействующие динамические объекты могут изменять параметры своей активности многократно, причем не только последовательно или пошагово, что является грубым допущением во многих теориях, например в теории игр, но и параллельно либо пересекаясь во времени, что требует новой корректировки вектора УВ $\bar{U}(\omega_i)$ всякий раз, когда претерпевает изменение вектор возмущения ω_i. Динамика такого рода изменений может быть весьма значительной. Усложняющим принятие решений ЛПР фактором является зависимость используемых метрик $\xi_1, \ldots, \xi_k$ от множества ненаблюдаемых или частично наблюдаемых параметров ПЦС и внешней среды, вследствие чего формализовать их с достаточной для целей управления точностью невозможно. Более того, метрики $\xi_1, \ldots, \xi_k$ дают динамические оценки, различные для каждой конкретной пары динамических объектов (A_0, A_i). Обычно их назначает ЛПР на основе собственного опыта и навыков с учетом текущей ситуации, что вносит значительную долю субъективности в процесс управления.

В ПЦС первого рода каждый из ЛПР динамического объекта $A_i \in \mathrm{A}^\chi$ решает задачу управления собственным динамическим объектом, поэтому задачу управления ПЦС в целом не ставят. В ПЦС второго рода для обеспечения взаимозависимости присутствует неявный или явный координатор, осуществляющий регулирование и ответственный за распределение активности динамического объекта во времени (т. е. планирование).

Осуществление координации может быть неформальным или формальным (таблица). Координацию неформальную строят на общих установках и стереотипах активности, требующих совместного согласованного взаимодействия.

Формы координации активности в ПЦС

Координация	Форма координации	
	Неявная	Явная
Неформальная	Добровольная, на уровне самоорганизации системы	С помощью решений нормативного регулятора или ответственного ЛПР (регулировщик)
Формальная	Добровольное выполнение нормативных предписаний (правила проезда нерегулируемого перекрестка)	С помощью нормативных процедур и правил нормативного регулятора (светофор)

При формальной координации задают множество правил. Нормативный регулятор (НР) осуществляет на регулирующие процесс взаимодействия взаимодействующие динамические процедуры $A_i \in \mathrm{A}^{\chi}$ координирующие воздействия $C_i, ..., C_m \in C$, устанавливая на основе наблюдаемых параметров состояния ПЦС отношения частичного порядка во времени и пространстве между элементами их активности, определяя тем самым их взаимные обязанности, приоритет и последовательность компенсации возмущений.

Необходимо отметить, что всякий нормативный регулятор (НР) в принципе является неполным и недоопределенным, а в некоторых ситуациях и противоречивым, что приводит к усложнению задач управления. Несмотря на наличие НР, действия ЛПР взаимодействующих динамических объектов являются во многом непредсказуемыми. Показано, что 82 % аварий на море происходит по вине человеческого фактора, из них 42 % связаны с намеренными, осознанными нарушениями операторов. Траектории их активности слабо прогнозируемы.

Рассматривая задачу управления на уровне ПЦС Ξ в целом, следует отметить, что соображения относительно управления динамическими объектами остаются справедливыми. Довольно часто саму динамическую систему рассматривают как динамический объект. В то же время размерность пространства C существенно возрастает, в результате чего число переменных состояния значительно превышает число наблюдаемых переменных. Стохастические воздействия внешней среды различны в разных точках области взаимодействия. Вследствие наличия нескольких взаимосвязанных каналов целенаправленного воздействия на состояние ПЦС последняя становится многомерной и многосвязной. К фундаментальным свойствам целеустремленных систем следует отнести:

- целенаправленность действий ЛПР по управлению (наличие *цели*);
- наличие у каждого ЛПР плана достижения своей цели, оптимального в схеме собственных (субъективных) установок;
- наличие возмущений выполняемых планов, требующих компенсации путем корректировки плана;
- взаимозависимость решений ЛПР взаимодействующих динамических объектов;
- непрогнозируемость (или слабую прогнозируемость) действий ЛПР;
- наличие НР совместной активности, в общем случае неполного и противоречивого (в системах второго рода);
- неопределенность f_U вследствие стохастического влияния внутренних и внешних воздействий, нестационарности и существенной нелинейности динамического объекта.

Формирование конкретного вектора УВ $\mathbf{U}(M)$ для выполнения компенсации $M(\omega_j)$ вследствие неопределенности f_U, а также необходимости во избежание критических ситуаций обеспечения согласования в системе критериев Q и ограничений R не является тривиальной задачей.

Целеустремленные динамические объекты могут отличаться видами и способами активности, масштабом, динамическими и инерционными характеристиками, целями и критериями функционирования. В формируемых ими ПЦС могут быть различными пространство совместной активности, выбранные нормы и соответствующие им метрики, временные шкалы и т. д. В то же время во всех полицелеустремленных системах наблюдаются общие свойства, принципы и способы управления, требующие формирования синхронизированных последовательностей УВ на ИУ взаимодействующих динамических объектов.

В полицелеустремленных системах ЛПР в процессе управления подвержено воздействию факторов неопределенности различной природы:

- неоднозначность реакции на УВ, прилагаемых к ИУ;
- непредсказуемость траектории активности в результате воздействий внешней среды и слабой прогнозируемости действий ЛПР;
- неточность исходной информации;

ненадежность и недостоверность оценки исходной информации как следствие ее отставания от реальной обстановки;

- нечеткость информации, имеющей лингвистическую природу ("недалеко", "совсем чуть-чуть" и т. д.), получаемой ЛПР по каналам зрительного, слухового, тактильного и т. д. наблюдения;
- неполнота исходной информации в связи с неполной наблюдаемостью системы и ограниченными возможностями УН и ЛПР;
- неоднозначность и противоречивость НР;
- недоопределенность оценки ситуации в присутствии ситуационных возмущений с изменяющимися элементами активности, являющаяся следствием непредсказуемости их дальнейшего поведения;
- субъективность выбираемых ЛПР решений и назначаемых им параметров УВ, подача которых зачастую вносит значительную долю субъективности как в процессе принятия решения, так и в процессе его передачи на ИУ.

Перечисленные свойства и факторы неопределенности/субъективности позволяют отнести ПЦС к классу слабоструктурированных, а проблемы управления ПЦС — к классу сложных и трудноформализуемых проблем. При наличии ЛПР целесообразно сводить проблемы управления к проблемам поддержки целенаправленного принятия решений.

Интроспективный анализ информационно-сложной ситуации

Таким образом, трудно-формализуемые проблемы принятия решений по управлению ПЦС в условиях информационно-сложных ситуаций (ИСС) значительно усложняются. В общем случае ЛПР динамического объекта имеет возможность анализировать ситуацию и своевременно принимать решения по компенсации различных возмущений [6]. В экстремальных случаях либо в условиях множественных ситуационных возмущений одновременно присутствует множество $\{\omega_i, ..., \omega_m\}$ возмущений, каждое из которых требует компенсации. Возникает дефицит времени, вызывающий напряженность при принятии решений, что под воздействием неблагоприятных психофизиологических факторов нередко приводит к ошибкам. Наличие множественных ситуационных возмущений требует выполнения сложных последовательностей их компенсаций. Если одновременно взаимодействует значительное число динамических объектов, ЛПР принимает решения в условиях неполной, неточной и недостоверной информации, а также значительной динамики, особенно в тех ситуациях, когда взаимодействующие динамические объекты интенсивно изменяют параметры активности, что требует своевременной корректировки и пересмотра процедур управления [4]. Кроме того, пространство поиска решений увеличивается, а пространство допустимых решений, наоборот, значительно сокращается, т. к. любой взаимодействующий динамический объект $A_i \in A^C$ является динамическим ограничением со слабо прогнозируемой траекторией активности для всех остальных $A_j \in A^C$, $A_j \neq A_i$. Информационно-сложную ситуацию (ИСС) для ЛПР определяют следующими условиями: дефицит времени на принятие решений; значительная динамика; существенное влияние факторов неопределенности и субъективности; увеличение продолжительности процедур принятия решений.

Продолжительность процедур принятия решений увеличивается за счет роста пространства поиска решений и числа действующих динамических ограничений, а также вследствие усложнения обработки исходной информации под действием ряда факторов неопределенности.

Дефицит времени, определяемый оценкой взаимодействия объектов с использованием временной метрики ξ_T, возникает, если оценка возмущения по временному критерию ξ_T имеет меньшее значение, чем оценка времени на принятие и выполнение решений по его компенсации, существенно ограничивает время на оценку обстановки и принятие решения, что вызывает противоречие со значительными объемами и сложностью обработки информации.

В ИСС ЛПР принимает решения на интуитивном уровне, полагаясь на свой опыт и навыки; его эвристические способности позволяют скомпенсировать неполноту и недостоверность информации, отсутствие или недостаточность формальных критериев, поэтому взаимодействующие динамические объекты подвергаются риску влияния "человеческого фактора", под воздействием которого в результате неправильных и непредсказуемых действий ЛПР происходит большинство инцидентов.

Таким образом, трудно формализуемые проблемы принятия решений по управлению полицелеустремленными системами в условиях ИСС значительно усложняются. Можно сделать следующие выводы об особенностях процесса принятия решений по управлению ПЦС:

- динамика внешних воздействий и ситуационных возмущений, изменяющаяся активность взаимодействующих динамических объектов приводят к необходимости динамической корректировки процедур управления;

- при запаздывании информации о параметрах состояния и элементах активности взаимодействующих динамических объектов ко времени принятия решения его принимают на основе неполной и неточной исходной информации, что усложняет данный процесс;
- принятие решений производят в условиях субъективности, так как большинство критериев, метрик, методов и процедур формализовать невозможно;
- для динамической корректировки процедур управления необходим анализ значительных объемов динамически меняющейся неточной и недостоверной исходной информации при существенных временных ограничениях на оценку обстановки и принятие решения и увеличении продолжительности процедур принятия решений, что приводит к возникновению информационно-сложных ситуаций;
- задачи управления в ИСС относятся к классу сложных и трудно формализуемых. Компенсация ситуационных возмущений, в особенности множественных, является наиболее сложной из задач управления ПЦС и требует обязательного участия ЛПР для принятия корректного и эффективного решения;
- в условиях ИСС современные методы не позволяют эффективно решать задачи управления ПЦС [6]. ЛПР принимают решения на основании субъективного опыта, знания закономерностей и соображений "здравого смысла" [2];
- подавляющее большинство опасных и критических ситуаций по управлению ПЦС складывается именно в ИСС, когда принятие решений ЛПР и без того существенно затруднено. Причины возникновения критических ситуаций в процессе управления динамическими объектами в большинстве случаев связаны с особенностями ЛПР, не соблюдающих установленные нормы и правила, игнорирующих меры предосторожности, не понимающих основные свойства и характеристики динамических объектов либо не осознающих степень опасности, которой они зачастую подвергают динамические объекты и ПЦС в целом своими действиями [5];
- для опасных и критических ситуаций характерно значительное уменьшение пространства допустимых решений и возможностей их корректировки под угрозой неполной управляемости или потери управляемости [1];
- в опасных и критических ситуациях наблюдается значительная зависимость результата управления от психофизиологического состояния ЛПР (человеческий фактор) [7, 8];
- ЛПР в процессе управления ПЦС сталкивается с повторяемостью принимаемых решений в сходных в определенной степени условиях (существует тесная взаимосвязь рассматриваемых ситуаций управления с пространством состояний ПЦС и классом динамического объекта) [1, 8, 9].

Детальный анализ условий формирования полицелеустремленных систем и возникновения информационно-сложных ситуаций, а также особенностей принятия решений в таких ситуациях

Можно сделать следующие выводы об особенностях процесса принятия решений по интроспективному синтезу ПЦС:

- динамика внешних воздействий и ситуационных возмущений, изменяющаяся активность взаимодействующих динамических объектов приводят к необходимости динамической корректировки процедур управления;
- при запаздывании информации о параметрах состояния и элементах активности взаимодействующих динамических объектов ко времени принятия решения его принимают на основе неполной и неточной исходной информации, что усложняет принятие решений;
- принятие решений производят в условиях субъективности, так как большинство критериев, метрик, методов и процедур формализовать невозможно;
- для динамической корректировки процедур управления необходим анализ значительных объемов динамически меняющейся неточной и недостоверной исходной информации при существенных ограничениях по времени на оценку обстановки и принятие решения и увеличении продолжительности процедур принятия решений, что приводит к возникновению информационно-сложных ситуаций;
- задачи управления в ИСС принадлежат к классу сложных и трудно формализуемых. Компенсация ситуационных возмущений, в особенности множественных, является наиболее сложной из задач управления ПЦС и требует обязательного участия ЛПР в принятии корректного и эффективного решения;
- в условиях ИСС современные методы не позволяют эффективно решать задачи управления ПЦС. ЛПР принимают решения на основании субъективного опыта, знания закономерностей и соображений здравого смысла;
- подавляющее большинство опасных и критических ситуаций по управлению ПЦС складыва-

ется именно в ИСС, когда принятие решений ЛПР и без того существенно затруднено;

- для опасных и критических ситуаций характерно значительное уменьшение пространства допустимых решений и возможностей их корректировки под угрозой неполной управляемости или потери управляемости;
- в опасных и критических ситуациях наблюдается значительная зависимость результата управления от психофизиологического состояния ЛПР (человеческий фактор);
- ЛПР в процессе управления ПЦС сталкивается с повторяемостью принимаемых решений в сходных условиях.

Литература

1. *Авдеева З. К., Коврига С. В., Макаренко Д. И.* Когнитивное моделирование для решения задач управления слабоструктурированными системами (ситуациями) // Управление большими системами. 2007. № 16. С. 26—39.
2. *Акофф Р., Эмери Ф.* О целеустремленных системах. — М.: ЛКИ, 2008. — 272 с.
3. *Алешин Б. С., Веремеенко К. К., Черноморский А. И.* Ориентация и навигация подвижных объектов. — М.: Физматлит, 2006. — 424 с.
4. *Быков Э. Б., Туркин И. И.* Самоорганизующиеся системы управления судовыми техническими средствами // Рациональное управление предприятием. 2007. № 1. С. 74—76.
5. *Вагин В. Н., Загорянская А. А.* Системы аргументации и абдуктивный вывод // Известия РАН. Теория и системы управления. 2004. № 1. С. 125—137.
6. *Вагин В. Н., Загорянская А. А.* Организация абдуктивного вывода средствами теории аргументации: Интеллектуальные системы / под ред. Курейчика В. М. — М.: Физматлит, 2005. С. 129—143.
7. *Дюбуа Д., Прад А.* Теория возможностей. Приложения к представлению знаний в информатике. — М.: Мир, 1990. — 288 с.
8. *Черный С. Г., Доровской В. А.* Методы и средства оценивания интроспективного мониторинга // Проблемы безопасности и чрезвычайных ситуаций. 2020. № 1. С. 75—87.
9. *Жиленков А. А., Черный С. Г.* Система безаварийного управления критически важными объектами в условиях кибернетических атак // Вопросы кибербезопасности. 2020. № 2(36). С. 58—66.

Synthesis of purpose systems in the conditions of information-complex situations

V. A. Dorovskoy, B. P. Novak, A. V. Degtyarev, A. S. Sobolev, P. A. Erofeev
Kerch State Maritime Technological University, Kerch, Russia

As a result of the study of organizational objects, a class of purposeful or purposeful systems was identified, taking into account basic goals that are set from the outside (usually this is the case in closed systems), and systems in which goals are formed within the system (which is typical for open, self-organizing systems). An introspective analysis and synthesis of purposeful systems in an information-complex situation with clearly expressed target aspirations to achieve the goal has been carried out. The investigated class of control systems for moving sea objects: ships and ships in information-complex situations and the activity of such systems is aimed at the result, and the result that is achieved in the presence of feedback.

Keywords: introspective analysis, introspective synthesis, purposeful systems, information-complex situation, multipurpose systems.

Bibliography — 9 references. *Received September 15, 2020*

УДК 004.932.72'1

Оптимизация искусственных нейронных сетей в задачах обработки графической информации для идентификации психофизиологических состояний субъекта

С. С. Жумажанова; *А. Е. Сулавко*, канд. техн. наук; *П. С. Ложников*, д-р техн. наук
ФГБОУ ВО "Омский государственный технический университет", г. Омск, Россия

Использование дистанционных технологий идентификации психофизиологических состояний (ПФС) субъекта необходимо. Применение таких систем имеет ряд преимуществ, связанных с возможностью осуществления скрытого контроля, с отсутствием физического контакта человека с системой и т. д. В связи с распространением коронавирусной инфекции COVID-19 индустрия безопасности находится в поиске способов использования имеющихся решений, в частности на базе тепловизионных камер, для их интеграции в системы массового скрининга субъектов. Это сделало очевидным тот факт, что тепловидение является альтернативным инструментом в борьбе с распространением эпидемии. Современные системы оценки ПФС человека имеют либо недостаточный функционал, связанный с ограниченным кругом идентифицируемых состояний, либо недостаточную точность идентификации состояний. Комплексирование различных методов обработки и преобразования цифровых изображений (термограмм), а также методов принятия решений на базе статистических и нейросетевых алгоритмов может решить указанную проблему. В настоящей работе приведены результаты исследований по идентификации нескольких психофизиологических состояний с использованием методов и алгоритмов обработки цифровых изображений и нейросетевого алгоритма принятия решений на базе комитета обученных сверточных нейронных сетей.

Ключевые слова: ИК-термография, термоизображения, психофизиологическое состояние, пространство признаков, формула гипотез Байеса, сверточные нейронные сети.

Система анализа и классификации человеческого фактора (HFACS) разработана доктором Скоттом Шаппеллом и доктором Дугом Вигманном [1]. Это широкая система человеческих ошибок, которую первоначально использовали ВВС США для исследования и анализа "человеческого фактора" в авиации (рис. 1).

В качестве такого фактора, как состояние оператора, в HFACS рассматривают неблагоприятные психические и физиологические состояния.

По данным международной статистики, основными причинами техногенных аварий являются усталость [2], сонливость [3], алкогольное опьянение [4], стресс [5].

Тепловые поля человека характеризуют температуру кожи, определяемую капиллярным кровотоком, изменения которого происходят под воздействием стимулов различного происхождения.

Жумажанова Самал Сагидулловна, аспирантка.
E-mail: samal_shumashanova@mail.ru
Сулавко Алексей Евгеньевич, доцент кафедры "Комплексная защита информации".
E-mail: sulavich@mail.ru
Ложников Павел Сергеевич, заведующий кафедрой "Комплексная защита информации".
E-mail: lozhnikov@gmail.com

Статья поступила в редакцию 23 сентября 2020 г.

Результаты по оценке состояния субъекта на основе параметров термограмм

Основная техническая характеристика биометрической системы — это ее точность (т. е. количество ложноположительных (FAR) и ложноотрицательных (FRR) решений, которые способна выдать система), что необходимо для достижения требуемых уровней безопасности. Другими словами, система характеризуется ошибками 1-го и 2-го рода. Для выявления недостатков текущих методов и алгоритмов идентификации ПФС по термограммам субъектов необходимо определить критерии их сравнения (табл. 1). В решаемых в данном исследовании задачах такими критериями являются:

- распознаваемые состояния: являются ли они степенью одного состояния (например, степень алкогольного опьянения или уровнями стресса) или абсолютно разными состояниями (сонливость, стресс);
- объем базы данных (БД), используемой для обучения и тестирования системы;
- точность метода/алгоритма;
- анализируемые области лица (лица и шеи) субъекта;
- идентификационные признаки.

Рис. 1. Структура HFACS

Таблица 1

Обзор последних работ по распознаванию ПФС

Автор/год	Регионы (ROI)	Объем БД (кол-во субъектов)	Признаки	Точность
Алкогольное опьянение				
Koukiou (2017) [6]	20 точек на лице	41	Значения пикселей в 20 точках	ИНС, 87 %
Hermosilla (2018) [7]	22 точки пересечения вен и капилляров на лице	8	Средняя интенсивность 3 × 3 пикселей вокруг каждой точки сетки	Байесовский классификатор на основе моделей гауссовой смеси, 87 %
Neagoe (2017) [8]	—	10	LDA-, PCA-признаки	Машина опорных векторов, SVM, 97,5 %
Koukiou (2018) [9]	Область лба	41	LDP-признаки	73—85 %
Сонливость				
Kiashari (2018) [10]	Область носа	12	Частота дыхания	95% (сравнение с контрольным методом)
Hu (2018) [11]	Область носа	12	Спектры мощности Фурье для частоты сердечных сокращений и частоты дыхания	81,3 и 95 % (сравнение с контрольным методом)
Физическая нагрузка				
Lopez (2017) [12]	Область лица	19	Признаки CHC	80 %, Alexnet и VGG
Стресс				
Sharma (2014) [13]	Область лица	35	Локальные двоичные шаблоны на дескрипторе трех ортогональных плоскостей (LBP—TOP), динамические тепловые диаграммы в гистограммах (HDTP)	86 %, SVM
Cho (2017) [14]	Область носа	8	Двухмерные спектрограммы вариабельности дыхания (RVS)	84,59 %, CHC
Engert (2014) [15]	Область лица	15	*N*-мерный вектор признаков	56 %, многомерный анализ паттернов (MPA)

Существуют значительные недостатки разработанных методов определения состояния по термограммам субъекта, например:

- системы имеют недостаточную точность либо низкую достоверность (малое число испытуемых) распознавания, подтвержденную экспериментально;
- в каждой из работ приведены результаты по идентификации только двух состояний, одно из которых является "нормальным", при этом не изучено насколько коррелируют тепловые образы лица человека в различных "измененных" состояниях;
- мало изучено влияние состояния усталости на тепловую картину лица и шеи для построения системы автоматической классификации данного состояния по термограмме.

Формирование базы термографических изображений субъектов

Разработана программа проведения натурных экспериментов по приведению субъектов в следующие состояния: "норма"; "алкогольное опьянение" (3 стадии); "стресс"; "физическая нагрузка"; "сонливость". Во время проведения опытов каждый испытуемый располагался в удобном кресле перед экраном монитора. Всего в экспериментах приняли участие 84 человека возрастом 18—28 лет. Производили съемку каждого субъекта на тепловизор Flir e60 в каждом из указанных состояний в разные дни.

Для определения того, находится ли субъект в состоянии «норма», проводились тесты по определению отклонений ЦНС (проба Ромберга, указательные пробы – пальценосовая, пальцепальцевая, ходьба по прямой линии и др.).

В текущих исследованиях идентифицировали три степени алкогольного опьянения: 0,2—0,29 ‰; 0,3—0,59 ‰; 0,6—0,9 ‰. Расчет необходимого количества алкоголя (в граммах) для достижения требуемой степени опьянения производили по формуле

$$M = \frac{p\, r\, m}{0{,}8 \cdot 0{,}9 \cdot g^2}, \qquad (1)$$

где M — масса (в граммах) алкоголя для достижения конкретного ВАС;
p — достигаемый уровень алкогольного опьянения в промиллях;
r — доля воды в мужском (0,7) или женском (0,6) организме;
m — масса тела;
0,8 — плотность спирта;
0,9 — всосавшегося в кровь спирта;
g — крепость выпитого алкоголя (в долях).

Для ввода субъекта в состояние психического (ментального) стресса использовали словесно-цветовой тест Струпа, который проводили в виде семи сессий, каждая длительностью 60 секунд с перерывами на отдых 30 секунд. Каждый испытуемый проходил тест на компьютере в специально разработанной для целей эксперимента программе.

Для ввода в состояние сонливости испытуемые принимали седативные средства (валериану, пустырник) согласно прилагаемой инструкции.

Также испытуемые выполняли физические упражнения (бег, отжимания и т. д.) пока частота сердечных сокращений не возрастала минимум на 30 %.

Разработан метод выделения 26 областей лица и шеи (с учетом информации об их антропометрическом и анатомическом строении). Из этих областей выделено 492 признака, характеризующих особенности распределения температуры на данных участках [16].

Для оценки качества полученных признаков необходимо определить их информативность. Под информативностью признака понимают то, насколько хорошо он характеризует распознаваемые образы. Чем выше информативность признака, тем с меньшей вероятностью ошибки данный признак позволяет разделить классы образов. При необходимости информативность можно представить в виде битов информации по формуле

$$I_{bit} = -\log_2 \bar{I} \qquad (2)$$

где $\bar{I} = 1 - I$; I — информативность признака, рассчитанная через площадь пересечения функций плотности вероятности значений признака, характеризующих, соответственно, классы образов (состояния) [17].

В результате выявлено, что большинство признаков является малоинформативными (рис. 2).

Произведено распознавание ПФС субъектов при помощи "наивного" классификатора Байеса. Распознавание ПФС в субъект-независимом режиме (когда обучение и тестирование происходят на термограммах разных испытуемых) позволило достичь точности 70 %, что не удовлетворяет требованиям, предъявляемым к таким системам. Таким образом, "наивная" схема классификации Байеса не подходит для задач распознавания ПФС с использованием термограмм, поскольку, кроме информативности, необходимо учитывать взаимную коррелированность признаков.

Рис. 2. Информативность всех признаков в битах

Построение архитектуры сверточной нейронной сети

Проведено экспериментальное исследование применимости аппарата сверточных нейронных сетей (СНС) для анализа и распознавания термографических образов человека. Предварительно обученные СНС могут быть использованы в качестве экстрактора признаков как часть стратегии передачи обучения (*transfer learning*) и классификатора входных данных по классам в зависимости от их целевой функции. В первом случае промежуточный выход предварительно обученной сети является непосредственно вектором признаков, который будет использован в качестве входных данных в новом классификаторе. СНС извлекают более сложные и абстрактные признаки, одновременно устраняя шумы изображения. Для стратегии передачи обучения предварительно обученную сеть используют в качестве отправной точки, которая затем настраивается с новыми образцами конкретного приложения (новых задач) для адаптации сети. Преимущество этого подхода состоит в использовании гораздо меньшего количества обучающих образов, чем при обучении сети с нуля. Кроме того, сеть обучается гораздо быстрее [18].

Чтобы сократить затраты на обучение решено вместо одной сети для идентификации всех ПФС использовать несколько сетей, каждая из которых обучается отличать определенное ПФС от состояния "норма" по предъявленному термографическому образу.

На вход СНС термографические образы подавали в виде исходных термографических изображений, а также вектора признаков, извлеченных из термограмм, и спектрограмм вектора признаков (рис. 3). Размерность термограмм равна разрешению изображения (240×320), соответственно, размерность входных данных для СНС в первом случае составляла 1, 240, 320. Значения пикселей предварительно нормировали на отрезке [0; 1].

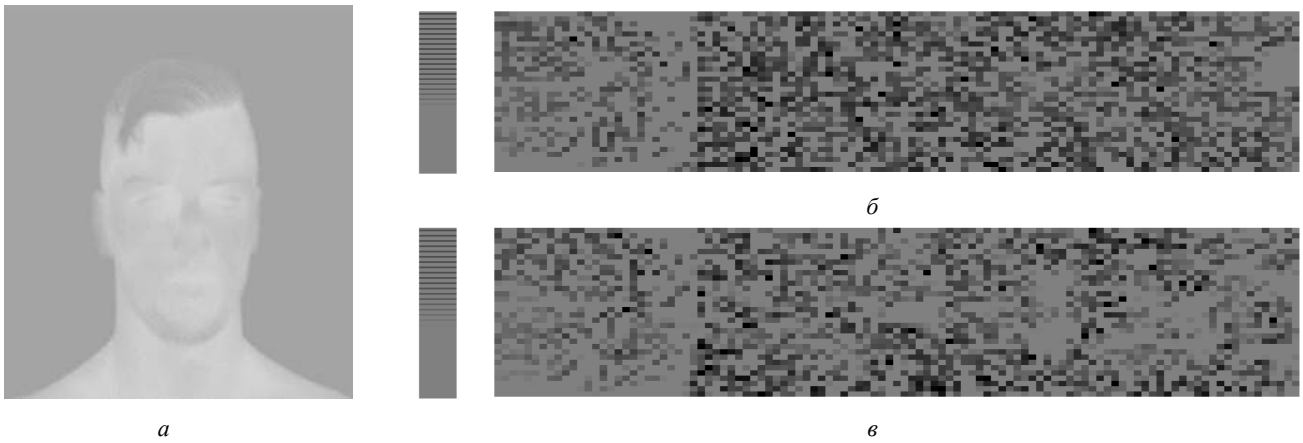


Рис. 3. Примеры входных данных:
а — термограмма, восстановленная из бинарного файла исходной термограммы для загрузки в модуль программы;
б — спектрограмма с типом окна Гаусса, шагом отчета 4 и размером окна 64 в состоянии "Норма";
в — спектрограмма с типом окна Гаусса, шагом отчета 4 и размером окна 64 в состоянии "Стресс"

В случае использования в качестве входных данных вектора признаков размерность составляла 1, 1, 492 (применялись СНС с одномерными свертками, а также были апробированы полносвязные сети). Особенностью такого решения является использование пары термограмм из соседних кадров для вычисления динамических признаков.

Размерность входных данных, подаваемых на вход СНС в виде спектрограмм, определяется размером окон Фурье и шагов отчетов. В целях уменьшения искажений в Фурье-анализе, вызванных малыми объемами выборки, к последовательности отсчетов участка сигналов применяют весовую функцию. В качестве весовой функции в данной работе использовали окна Хэмминга, Блэкмана, Барлетта (треугольное окно), Гаусса, Лапласа, прямоугольное окно, параметрическую Гауссиану. В настоящем исследовании использовали 7 окон Фурье по отдельности. Спектрограммы вычисляли с окнами Фурье размера 16, 32, 64 и шагами 2, 4, 6, 8 и 10 отчетов. Амплитуды образов были нормализованы на отрезке [0; 1]. Нормировку проводили по минимуму и максимуму показателей амплитуд всех сигналов для всех испытуемых. Рассматривали шесть базовых архитектур СНС, приведенных на рис. 4, обозначения к которому представлены в табл. 2.

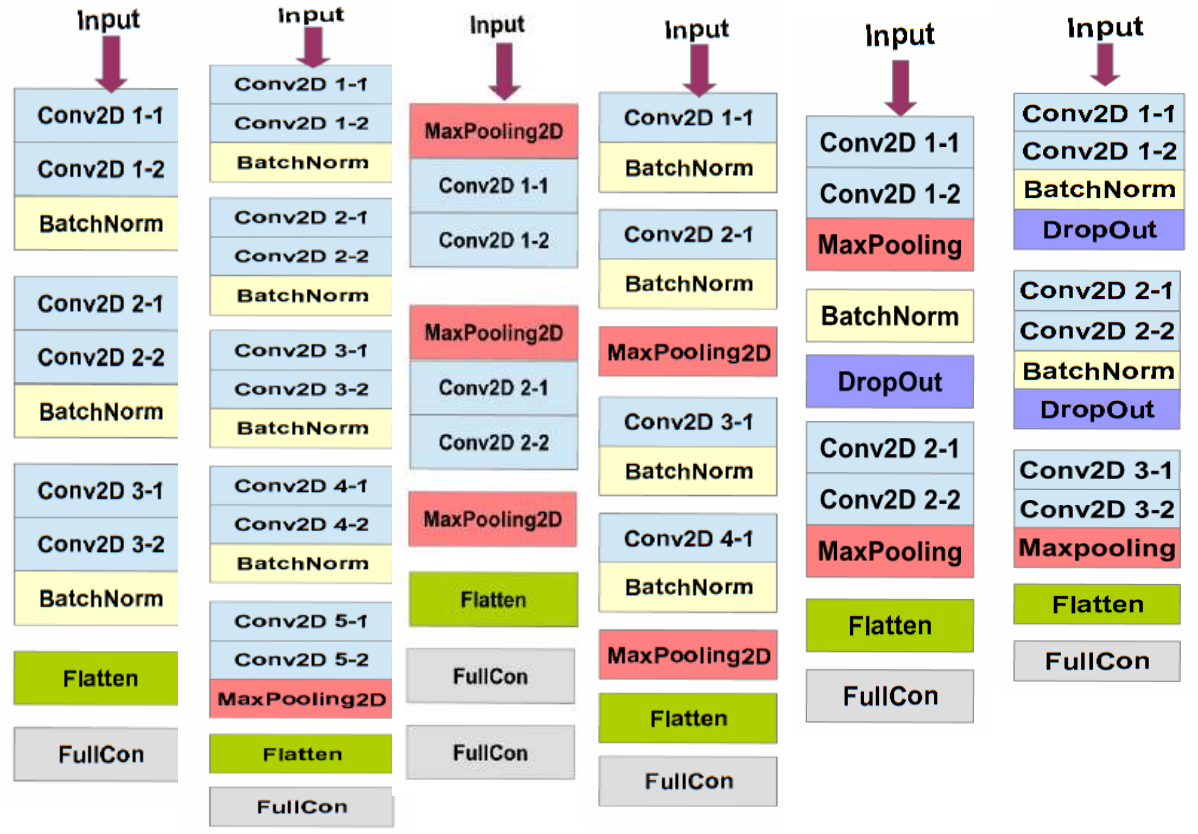


Рис. 4. Архитектуры используемых СНС под номерами № 1—6 (слева направо)

Таблица 2

Обозначения структурных блоков СНС

Обозначение	Название	Параметры
Input	Входной слой	Размерность входных данных
Conv2D	Сверточный слой	Количество фильтров, размерность страйда, функция активации, метод инициализации весов
MaxPooling2D	Пулинговый слой по максимуму	Размер пула, размерность страйда
Flatten	Слой выравнивания (выпрямления)	
FullCon	Полносвязный слой	units (количество нейронов), activation (функция активации), метод инициализации весов
BatchNorm	Слой нормализации по мини-батчам	
DropOut	Слой субдискретизации	

Результаты вычислительного эксперимента

При обучении и тестировании использовали объемы выборок, указанные в табл. 3. Использование входных данных в виде термограмм размерностью (1, 240, 320) и в виде векторов признаков для распознавания ПФС на базе представленных СНС не дало удовлетворительных результатов по точности распознавания.

Таблица 3

Параметры обучения СНС (объемы выборки на класс)

Класс	Объем выборки
Обучающей	2010 (67×30)
Валидационной	68
Тестовой	420

Для каждой архитектуры сетей, принимающих в качестве входных данных спектрограммы вектора признаков, выбрана наиболее "успешная" с точки зрения эффективности (более высокая средняя точность и меньшая размерность спектрограммы) пара "окно–шаг". Обучали не все возможные комбинации, а часть. Сначала устанавливали тип и размер (начиная с 16) окна, затем изменяли шаг, начиная с 10. Процесс останавливали при отсутствии существенного роста точности решений на валидационной выборке. Далее аналогично итерационно изменяли размер окна. Из апробированных комбинаций выделено 30 архитектур, которые протестированы с использованием тестовой выборки. Результаты (табл. 4), полученные для избранных конфигураций СНС, не отвечают требованиям, предъявляемым к таким системам.

Из 30 конфигураций для каждого ПФС выбраны 5 наиболее эффективных СНС в плане точности распознавания, которые объединены в ансамбли (комитеты). Идея объединения СНС в комитет основана на теореме Кондорсе: чем выше вероятность верного решения для каждой СНС в отдельности, тем выше вероятность верного решения комитета (при условии, что каждая сеть дает точность более 50 %).

Таблица 4

Результаты по идентификации ПФС

ПФС	Средняя точность распознавания ПФС	Максимальное значение точности распознавания ПФС	Минимальное значение точности распознавания ПФС
Норма	0,59	0,64	0,56
Первая стадия алкогольного опьянения	0,6	0,66	0,54
Вторая стадия алкогольного опьянения	0,63	0,69	0,58
Третья стадия алкогольного опьянения	0,68	0,72	0,57
Стресс	0,85	0,94	0,79
Физическая усталость	0,7	0,74	0,65
Сонливость	0,58	0,63	0,55

Важна также степень коррелированности решений сетей. Чем она ниже, тем более выражен синергетический эффект от их объединения. При этом каждая архитектура в сочетании с определенным типом окон может входить в комитет неоднократно, так как при повторном обучении "с нуля" одной и той же архитектуры на тех же данных возникают две различные обученные сети (с разными весовыми коэффициентами). Решения этих сетей будут не полностью коррелированы. Назовем такие сети дублерами.

Рассчитана точность распознавания каждого ПФС в отдельности в зависимости от того, сколько дублеров каждой сети вошло в комитет (рис. 5).

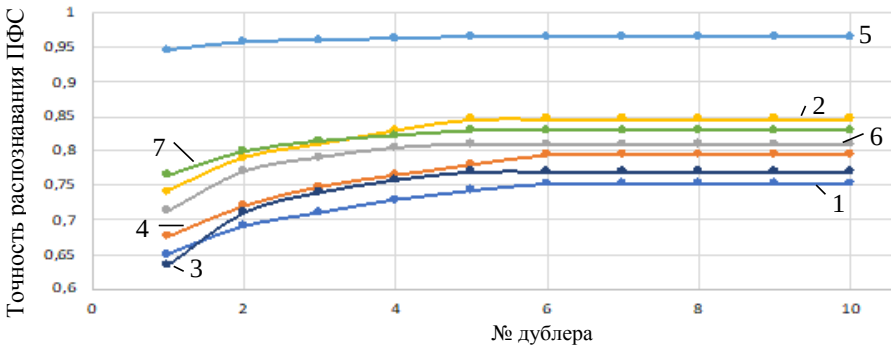


Рис. 5. Результаты верификации ПФС при объединении СНС в ансамбли

1 — норма; 2 — 3-я стадия алкогольного опьянения; 3 — сонливость; 4 — 1-я стадия алкогольного опьянения; 5 —стресс; 6 —2-я стадия алкогольного опьянения; 7 —физическая усталость

Объединения решений достигали путем усреднения выходов сети, ассоциированных с уровнем схожести образа с определенным ПФС. Установлено, что предложенный способ усреднения результатов решений дает более высокую точность распознавания, однако при количестве дублеров более 6 существенного повышения точности не обнаружено. Наилучшие результаты показали СНС, обученные на распознавание состояния "стресс".

Заключение

Обзор работ по распознаванию психофизиологического состояния субъектов по термографическим изображениям лица и шеи показал, что имеющиеся результаты не отвечают требованиям практики. Рассмотрены архитектуры сверточных искусственных нейронных сетей в задачах распознавания ПФС по термографическим изображениям. Предложен метод преобразования термограммы в компактную и информативную спектрограмму путем вычисления вектора 492 признаков и применения к нему быстрого оконного преобразования Фурье. Вычислительный эксперимент показал, что надежность распознавания и скорость обучения возрастают, если в качестве входных данных использовать спектрограммы.

Произведено объединение СНС в комитеты по 5 штук, рассчитана точность распознавания ПФС при отсутствии дублеров СНС и постепенном увеличении числа дублеров. Вычислительный эксперимент показал, что подобное усреднение решений ансамблей сети дает более высокие результаты по распознаванию ПФС при наличии 5—6 дублеров в зависимости от ПФС. Дальнейшее увеличение числа дублеров не дало значительного улучшения результатов. Наилучшие показатели точности продемонстрировали СНС, обученные на распознавание состояния "Стресс".

Дальнейшие работы в данном направлении стоит акцентировать на создание метода непрерывной идентификации ПФС, который будет компенсировать решения комитетов СНС, что можно сделать путем последовательного применения формулы гипотез Байеса.

Литература

1. HFACS, Inc | The HFACS Framework [Электронный ресурс]. URL: https://www.hfacs.com/hfacs-framework.html (дата обращения: 18.10.2019).
2. Driver fatigue and road accidents — RoSPA [Электронный ресурс]. URL: https://www.rospa.com/road-safety/advice/drivers/fatigue/road-accidents/ (дата обращения: 07.10.2019).
3. Prevalence of Drowsy Driving Crashes: Estimates from a Large-Scale Naturalistic Driving Study [Электронный ресурс] // AAA Foundation. 2018. URL: https://aaafoundation.org/ prevalence-drowsy-driving-crashes-estimates-large-scale-naturalistic-driving-study/ (дата обращения: 08.10.2019).
4. lynn.greenbauer.ctr@dot.gov. Driving Drunk or High Puts Everyone in Danger [Электронный ресурс]: Text // NHTSA. 2017. URL: https://www.nhtsa.gov/drunk-driving/drive-sober-or-get-pulled-over (дата обращения: 08.10.2019).
5. The Effects of a Heavy Workload on Employees [Электронный ресурс] // Bizfluent. URL: https://bizfluent.com/info-8178431-effects-heavy-workload-employees.html (дата обращения: 08.10.2019).
6. **Koukiou G.** Intoxication Identification Using Thermal Imaging // Hum.-Robot Interact. - Theory Appl. 2017.
7. **Hermosilla G. et al.** Face Recognition and Drunk Classification Using Infrared Face Images [Электронный ресурс]: Research article // J. Sensors. 2018. URL: https://www.hindawi.com/journals/js/2018/5813514/ (accessed: 04.09.2019).
8. **Neagoe V.-E., Carata S.-V.** Drunkenness diagnosis using a Neural Network-based approach for analysis of facial images in the thermal infrared spectrum // 2017 E-Health Bioeng. Conf. EHB. 2017. P. 165—168.
9. **Koukiou G., Anastassopoulos V.** Local difference patterns for drunk person identification // Multimed. Tools Appl. 2018. V. 77. № 8. P. 9293–9305.
10. **Kiashari S. E. H. et al.** Monitoring the Variation in Driver Respiration Rate from Wakefulness to Drowsiness: A Non-Intrusive Method for Drowsiness Detection Using Thermal Imaging // J. Sleep Sci. 2018. V. 3. № 1–2. P. 1–9.
11. **Hu M. et al.** Combination of near-infrared and thermal imaging techniques for the remote and simultaneous measurements of breathing and heart rates under sleep situation // PloS One. 2018. V. 13. № 1. P. e0190466.
12. **Lopez M. B., del-Blanco C. R., Garcia N.** Detecting exercise-induced fatigue using thermal imaging and deep learning: 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA). 2017. P. 1–6.
13. **Sharma N. et al.** Thermal spatio-temporal data for stress recognition // EURASIP J. Image Video Process. 2014. V. 2014. № 1. P. 28.
14. **Cho Y., Bianchi-Berthouze N., Julier S. J.** DeepBreath: Deep Learning of Breathing Patterns for Automatic Stress Recognition using Low-Cost Thermal Imaging in Unconstrained Settings // 2017 Seventh Int. Conf. Affect. Comput. Intell. Interact. ACII. 2017. P. 456–463.
15. **Engert V. et al.** Exploring the Use of Thermal Infrared Imaging in Human Stress Research // PLoS ONE. 2014. V. 9. № 3.
16. **Жумажанова С. С., Лукин Д. В., Белгородцев А. А.** Разработка методики выделения участков лица и шеи на термограммах и изображениях в видимом спектре для последующего анализа в целях выявления психофизиологического состояния субъекта (Обзор) // Вопросы защиты информации. 2018. № 4. С. 24—35.
17. **Сулавко А. Е., Жумажанова С. С., Фофанов Г. А.** Перспективные нейросетевые алгоритмы распознавания динамических биометрических образов в пространстве взаимозависимых признаков // Динамика систем механизмов и машин. 2018. V. 6. № 4.
18. **Николенко С., Кадурин А., Архангельская Е.** Глубокое обучение. – СПБ: Издательский дом "Питер, 2017. — 481 с.

Analysis of face and neck thermograms for users' drowsiness recognition based on the Bayesian classifier

S. S. Zhumazhanova, A. E. Sulavko, P. S. Lozhnikov
Omsk State Technical University, Omsk, Russia

The use of remote technologies for psychophysiological deviations (PPS) identification is currently necessary. The use of such systems has a number of advantages associated with the absence of damage while collecting information about the state of the subject, physical contact of a person with the system, etc. In connection with the spread of the coronavirus infection COVID-19, the security industry is looking for ways to use existing solutions, in particular, based on thermal imaging cameras, for their integration into subjects mass-screening systems. It makes it clear that thermal imaging is an alternative tool in the fight against the spread of the epidemic. Modern systems for assessing human PPS have either insufficient functionality associated with a limited range of identifiable states, or insufficient accuracy in identifying states. The integration of various methods of processing and transforming digital images (thermograms), as well as decision-making methods based on statistical and neural network algorithms, can solve this problem. This article presents the results of studies on identification of several psychophysiological states using methods and algorithms for processing digital images and a neural network decision-making algorithm based on a committee of trained convolutional neural networks.

Keywords: IR thermography, thermal images, psychophysiological state, feature space, Bayesian hypothesis formula, convolutional neural networks.

Bibliography — 18 references. *Received September 23, 2020*

УДК 004.056.5

Модели оценки риска нарушений информационной безопасности при эксплуатации систем охраны исправительных учреждений

Д. В. Титов, канд. техн. наук; *Е. Е. Филипова*, канд. физ.-мат. наук
ФКОУ "Вологодский институт права и экономики ФСИН России", г. Вологда, Россия

Рассмотрены критерии и методы оценки риска нарушений в работе систем безопасности для выбора оптимального решения в построении интегрированных систем безопасности в учреждениях уголовно-исполнительной системы.

Ключевые слова: интегрированная система безопасности, промышленная автоматизация, многоуровневая система сбора и обработки информации, критерий, методы оценки рисков, техническая система, надежность, информационная безопасность.

В учреждениях и органах уголовно-исполнительной системы (УИС) внедрены и успешно функционируют автоматизированные системы охраны. Их принято называть интегрированными системами безопасности (ИСБ). Эксплуатация ИСБ в учреждениях регламентирована нормативно-правовой базой [1, 2].

Для обеспечения задач охраны и надзора активно применяются такие ИСБ, как "Тобол", "Пахра", "Микрос-02", "Рубеж-08", "Синергет" и т. д. Все они осуществляют сбор, обработку и передачу информации. В соответствии с подходами к построению систем промышленной автоматизации систему сбора и обработки информации принято представлять в виде пирамиды уровней, связанных шинами данных и шинами управления, с указанием преобразователей интерфейсов и портов устройств. Структура подобных систем с выводами подробно рассмотрена в работе [3].

Необходимо отметить, что в любом случае применяемая модель должна иметь достаточный уровень адекватности реальному объекту [4]. Таким образом, критериями выбора к внедрению данных систем на объектах охраны исправительных учреждений могут являться следующие:

- Количество обслуживаемых портов, типы промышленного интерфейса и протокола обмена данными.
- Скорость обработки, а также объем сохраняемой во внешней памяти устройств сбора данных информации о сигналах с датчиков обнаружения.
- Устойчивость линии к внешним помехам, надежность передачи, энергозависимость.
- Стоимость проекта и смета расходов на установку системы. Данный критерий имеет большое значение и оказывает большое влияние на выбор поставщика и сроки установки ИСБ в учреждении.
- Критерий безопасности. Все используемые протоколы, устройства и программное обеспечение должны соответствовать требованиям по обеспечению информационной безопасности.

Рассмотрим обеспечение информационной безопасности с точки зрения устойчивости интегрированной системы безопасности к внешним воздействиям. Известно, что безопасность промышленного объекта — это состояние его защищенности от различных угроз, при котором созданы условия для нормального функционирования и строгого соблюдения установленных режимов. Поскольку, как уже отмечалось, ИСБ можно представить в виде системы промышленной безопасности, будем использовать соответствующую терминологию.

Таким образом, модель оценки рисков нарушений работы (отказов) промышленной системы априори является моделью оценки уровня информационной безопасности. Показатели оценки указанных рисков определяют экспертными методами, позволяющими избежать необходимости накопления статистических данных об учитываемых факторах рисков.

Количественная оценка рисков представляет собой совокупность регулярных процедур анализа риска, идентификации источников его возникновения, определения возможных масштабов

Титов Дмитрий Валерьевич, доцент кафедры "Информатика и математика" факультета психологии и права.
E-mail: titov_dv@mail.ru
Филипова Елена Евгеньевна, доцент кафедры "Информатика и математика" инженерно-экономического факультета.
E-mail: lenphil@mail.ru

Статья поступила в редакцию 25 сентября 2020 г.

последствий проявления факторов риска, а также роли каждого источника в общем профиле риска.

Методы оценки рисков являются основой исследований в обеспечении безопасности объектов и выбора методов управления ими в конкретных условиях. Для определения количественной оценки рисков обычно применяют два основных методических подхода:

- расчетный, заключающийся в прогнозировании ущерба на основе априорных данных о возможности появления рисковых событий;
- вероятностный, базирующийся на определении вероятности наступления рисковых событий и оценке размеров предполагаемых последствий.

В общем случае все сбои в аппаратно-программных средствах интегрированных систем безопасности можно разделить на несколько классов:

- аппаратные сбои обеспечения компьютеров в составе ИСБ (дежурная часть);
- сбои и неполадки, вызванные несовместимостью отдельных устройств, версий драйверов и т. п.;
- сбои и неполадки, вызванные несоблюдением условий эксплуатации технических средств охраны;
- сбои и неполадки, вызванные неисправностью устройств;
- перегрев оборудования из-за отсутствия охлаждения;
- статический разряд от прикосновения к отдельным элементам или системному блоку в целом;
- скачкообразное и (или) повышенное напряжение питания в электросети, к которой подключены технические средства охраны и надзора (например, разряд молнии).

В качестве примера оценки риска сбоев (отказов) приведем метод оценки надежности сложной технической системы. Выберем в качестве показателя надёжности технической системы функцию вероятности безотказной работы $P(t)$. Эта функция численно определяет вероятность нормального функционирования технической системы (в нашем случае — ИСБ) в течение некоторого времени t при условии, что в заданном интервале времени $[t=T]$ не возникнет отказа системы. Значение функции $P(t)$ может находиться в пределах $0 \le P(t) \le 1$. Сумма вероятностей безотказной работы системы $P(t)$ и отказа $R(t)$ равна 1, так как эти события образуют полную группу событий. Поэтому в качестве простейшего математического аппарата оценки рисков используем формулу

$$P(t) + R(t) = 1. \quad (1)$$

В теории надежности используют различные законы распределения. Для решения задач, связанных с прогнозированием отказов интегрированных систем безопасности в гарантийный промежуток времени, подойдет экспоненциальный закон распределения, называемый также основным законом надёжности [5].

Рассмотрим примеры неблагоприятного сочетания условий работы, вызывающих внезапный отказ. Для интегрированных систем и комплексов безопасности такими факторами риска выступают внешние воздействия — превышение допустимого тока через цепи устройства (короткое замыкание) и нарушение температурного режима (перегрев, ложные срабатывания).

Плотность распределения экспоненциального закона описывается соотношением

$$f(x) = \lambda t^{-\lambda x}. \quad (2)$$

Кроме того, определяют:

- функцию распределения

$$F(x) = 1 - e^{-\lambda x}; \quad (3)$$

- функцию надёжности (распределения вероятности)

$$P(x) = 1 - F(x) = e^{-\lambda x}; \quad (4)$$

- математическое ожидание случайной величины x

$$M(x) = \lambda \int_0^\infty x e^{-\lambda x} dx = \frac{1}{\lambda}; \quad (5)$$

- дисперсию случайной величины x

$$D(x) = \lambda \int_0^\infty x^2 e^{-\lambda x} dx - \frac{1}{\lambda^2} = \frac{1}{\lambda^2}. \quad (6)$$

Заключение

Своевременное использование моделей для оценки риска нарушений информационной безопасности позволяет выявлять слабые стороны в

построении интегрированных систем безопасности конкретного учреждения. Набор внутренних параметров модели должен содержать прежде всего географические, конструктивные особенности режимного объекта. В противном случае возрастает риск отказов систем автоматизации и (или) снижается их эффективность. От этих факторов зависит выполнение важнейших задач: сохранения необходимого уровня защиты информации и соблюдения режима охраны и безопасности.

Литература

1. Приказ Министерства юстиции РФ от 17 июня 2013 г. № 94 «О внесении изменений в приказ Министерства юстиции Российской Федерации от 4 сентября 2006 г. № 279 «Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы».

2. Об утверждении Руководства по технической эксплуатации инженерно-технических средств охраны и надзора, применяемых для оборудования объектов уголовно-исполнительной системы: приказ ФСИН России от 18.08.2006 г. № 574 // Ведомости уголовно-исполнительной системы. 2007. № 5—7.

3. *Титов Д. В., Данилов А. В.* Критерии выбора интегрированных систем безопасности для обеспечения задач охраны исправительных учреждений // Современные средства автоматизации деятельности сотрудников территориальных органов и образовательных организаций ФСИН России: проблемы и перспективы: сб. матер. научно-практического семинара. Вологда, 24.10.2019 / под. ред. Бабкина А. А. — Вологда: ВИПЭ ФСИН России, 2020. – 178 с.

4. *Саати Т. Л.* Принятие решений: Метод анализа иерархий / Пер. с англ. — М.: Радио и связь, 1993. – 314 с.

5. *Шубин Р. А.* Надёжность технических систем и техногенный риск: уч. пособие / — Тамбов: Изд-во ФГБОУ ВПО "Тамбовский государственный технический университет", 2012. — 80 с.

Models for assessing the risk of information security violations during the operation of correctional security systems

D. V. Titov, E. E. Filipova
Vologda Institute of Law and Economics of the Federal Penitentiary Service of Russia,
Vologda, Russia

This work considers the criteria and methods for assessing the risk of violations in the operation of security systems in order to choose the optimal solution in the construction of integrated security systems in institutions of the penal system.

Keywords: integrated security system, industrial automation, multilevel information collection and processing system, criteria, risk assessment methods, technical system, reliability, information security.

Bibliography — 5 references. *Received September 25, 2020*

УДК 004.772

Методы обфускации сетевого трафика

А. О. Неволин, канд. техн. наук
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Рассмотрены проблемы скрытой передачи данных в современных телекоммуникационных сетях (прежде всего, Интернет). Предлагается способ завуалированного информационного обмена без использования шифрования. Описываются меры противодействия существующим системам DPI.

Ключевые слова: шифрование, Tor, информационная безопасность, завуалированный информационный обмен, обфускация трафика.

Нет сомнений в важности информации. Владение нужной информацией зачастую является ключевым фактором победы в каких-либо противостояниях, начиная от конкуренции бизнес-компаний и заканчивая военными действиями. Поэтому крайне высок уровень "охоты" за информацией — попыток узнать конфиденциальную информацию несанкционированным получателям.

Одно из наиболее уязвимых звеньев, при которых происходит похищение информации, — момент ее передачи от отправителя к получателю. Для информационного обмена используют телекоммуникационные сети, как локальные, так и глобальную сеть Интернет. Для защиты данных на этом этапе применяют различные решения, которые развивались по мере эволюционирования средств информационной борьбы.

Первым "эшелоном", активно используемым до сих пор, были сетевые экраны (которые так же называют браундмауэрами или файрволами, от английского общепринятого слова firewall). Общий принцип их работы заключается в блокировании сетевого соединения по тем или иным признакам. Простейшие брандмауэры (например, встроенный в операционную систему Windows [1]) блокируют соединения лишь по номеру используемого порта. Более сложные сетевые экраны используют более продвинутые критерии анализа, например, простейший анализ заголовков пакетов, общая сетевая активность источника и др.

Неволин Александр Олегович, доцент кафедры «Радиосистемы и комплексы управления, передачи информации и информационная безопасность».
E-mail: nevolin.ao@yandex.ru

Статья поступила в редакцию 26 сентября 2020 г.

Следующим этапом развития стало появление систем DPI — Deep Packet Inspection. Такие средства по сути являются глубокой модернизацией самых развитых брандмауэров. Ключевое их отличие — это то, что они анализируют как заголовки, так и содержимое пакетов. Кроме того, применяется не только поиск по сигнатуре, но и анализ статистических характеристик передаваемых данных. Конечная цель инструментов DPI — определение типа используемого протокола и извлечение конкретной информации.

Для защиты от DPI наиболее часто применяют шифрующие протоколы (TLS и другие). Несмотря на то, что в целом шифрование не только полностью разрушает видимую структуру данных, но и "выравнивает" ее статистические характеристики, все равно остаются косвенные признаки, которые могут быть использованы для определения протокола. Так, например, в Эфиопии было заблокировано использование протокола Tor (использующего тройное шифрование) с помощью средств DPI.

Также огромным недостатком шифрования является неизбежное привлечение внимания третьей стороны. Поэтому в случае необходимости скрытой передачи информации в условиях применения противником средств DPI использование шифрования несет в себе большие риски обнаружения.

Кроме того, наравне с инструментами DPI появились системы обнаружения вторжений (IDS — Intrusion Detection System), системы обнаружения утечек данных (DLP — Data Leakage Protection), системы предотвращения вторжений (IPS — Intrusion Prevention System) и другие аналогичные системы. Эти системы также используют анализ статистических характеристик трафика для обнаружения фактов вторжения или утечки данных. Последней тенденцией становится применение в таких системах нейронных сетей.

Имеются также работы по анализу зашифрованного трафика (например, тот же TLS) по статистическим характеристикам низкого уровня: на уровне транспортного протокола анализируются задержки между пакетами, их число и др. В работе описывается подход, позволяющий полностью сымитировать данные характеристики.

Предлагается альтернативный метод защиты передаваемых данных, получивший название "обфускации" — по аналогии с обфускацией программного кода, используемой на платформах с компиляцией в промежуточные языки программирования (Java, .Net) [2].

Общая структура протоколов

Все приводимые далее выкладки будем считать применяемыми для протоколов прикладного уровня [3], т. к. именно там сегодня наблюдаются наиболее активные попытки похищения информации. Кроме того, все протоколы более низких уровней достаточно стандартизированы и маловероятно появление каких-либо новых форматов.

Основной сутью предлагаемого метода является маскировка одного протокола (назовем его исходным) под другой (назовем его маскирующим), например, трафик по протоколу HTTP может быть замаскирован под трафик FTP. При этом необходимо соблюдение ключевого условия – соответствия статистических характеристик маскирующего протокола реальному, поскольку многие инструменты DPI активно применяют такой анализ. Другими словами, при маскировке HTTP под FTP необходимо обеспечить, чтобы внешне статистические характеристики получившегося FTP отличались от реального FTP на величину меньшую, чем порог обнаружения DPI-инструментов.

Для того, чтобы описать метод более подробно, попытаемся сначала составить типовую структуру большинства протоколов прикладного уровня.

Если провести подобный анализ, то обнаружится, что практически во всех таких протоколах используют команды. В целом, как правило, каждая команда имеет:

- обозначение (код или название);
- входные параметры (приходят от отправителя);
- выходные параметры (возвращаются отправителю).

Общий перечень команд известен и задокументирован в спецификации соответствующего протокола.

Любой параметр (как входной, так и выходной) должен иметь какой-либо адресный признак и значение.

Адресным признаком может являться как конкретное местоположение параметра в пакете (например, с 481 по 495-й байты), так и название (например, параметр Content-type в протоколе HTTP).

Больший интерес представляют возможные значения параметров. Их условно можно разделить на два вида:

- имеющие конечное число значений;
- имеющие бесконечное число значений (как правило, это бинарные данные).

Рассмотрим более подробно конечные значения, поскольку именно они более удобны для использования в обфускации. Под конечными значениями наиболее часто стоит понимать:

- Число (цифра) — конечным значением его можно считать потому, что, как правило, по стандарту протокола число может лежать только в определенном диапазоне, а следовательно – количество вариантов конечно.
- Дата;
- Одно значение из нескольких фиксированных (некий аналог Enum из языков программирования);
- Строка (поскольку длина строки, как правило, ограничена, то количество возможных вариантов тоже конечно).

Таким образом, у конечных параметров всегда можно определить количество возможных значений (или "размер алфавита" в терминах теории информации). Эта информация далее будет использована для самого процесса обфускации.

Предварительный анализ протоколов

Используя описанные выше критерии, для каждого имеющегося сегодня протокола можно составить его «портрет», который выражается в описании команд, для каждой из которых указывается:

- перечень ее параметров;
- количество возможных комбинаций значений каждого из параметров.

Данные сведения позволяют составить "карту" протокола. Для всех распространенных протоколов получение подобной карты не представляет большого труда — для этого необходим анализ спецификации протокола и, в некоторых случаях, анализ реального трафика.

Процедура обфускации

В целом обфускация протокола состоит из следующих блоков:

- подбор маскирующего протокола;
- генерация схемы кодирования;

Отправитель, желая передать данные в обфусцированном виде, сначала должен подобрать маскирующий протокол. Для этого необходимо перебрать каждый из маскирующих протоколов и сгенерировать схему кодирования для каждой подобной связки.

Фактически кодирование исходного протокола на маскирующий осуществляется трансляцией значений параметров одного протокола на параметры другого. В качестве примера процесс трансляции показан на рисунке.

В данном примере параметр исходного протокола с условным №2, имеющий 10,600 возможных значений, распределяется на параметры с условными номерами №1, №3 и другие параметры маскирующего протокола. Таким образом, часть значений параметра исходного протокола транслируется на один параметр маскирующего, часть – на другой, и т. д. В случае, если у параметров близкое число возможных значений, их можно транслировать 1-в-1 (параметр-в-параметр).

Подобная трансляция неизбежно вызовет изменение статистических характеристик маскирующего протокола по сравнению с реальным. Обозначим такое изменение как *delta*. Предположим, что инструмент DPI будет пытаться обнаружить подмену протокола именно по мере отличия его статических характеристик от общеизвестных. Логично предположить, что при этом у инструмента будет задан некоторый порог срабатывания *threshold*. Это вызвано тем, что в реальной среде протоколы имеют определенную вариативность статистических характеристик, которую необходимо учитывать для исключения ложных срабатываний (false positive).

Таким образом, для исключения обнаружения факта маскировки протокола достаточно подобрать такой протокол и схемы кодирования, чтобы:

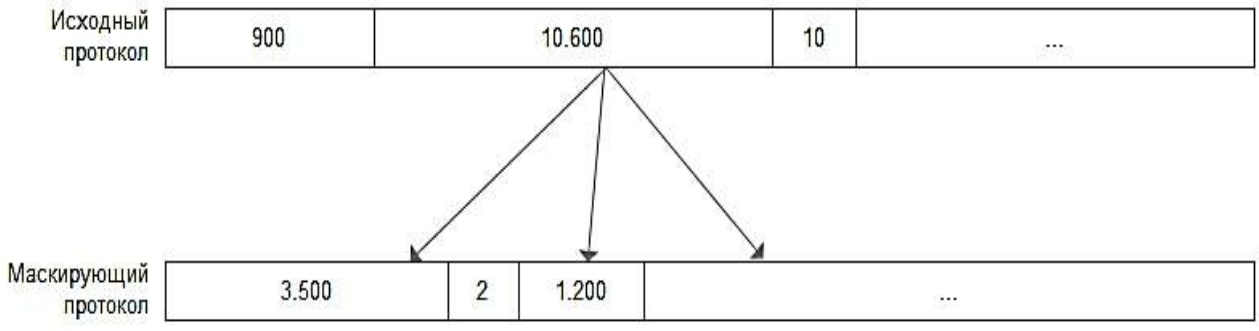
$$delta < threshold$$

В реальных условиях значение *threshold* неизвестно (поскольку оно задано на уровне настроек DPI-инструмента, которые, как и методика вычисления статистических отличий, нам неизвестны), поэтому для осуществления информационного обмена наилучшей стратегией будет выбор маскирующего протокола, у которого при имеющейся схеме обфускации значение *delta* будет минимальным по сравнению с другими протоколами.

Также возможно использование различных схем трансляции параметров в рамках одной пары «исходный протокол — маскирующий протокол». Разные схемы могут давать разное изменение статистических характеристик протокола (меру *delta*), поэтому имеет смысл не только перебирать различные маскирующие протоколы, но и пробовать различные схемы трансляции.

Возможен более интеллектуальный выбор параметров для трансляции. Например, имеет смысл числовые параметры транслировать в числовые, перечисляемые — в перечисляемые и др. В некоторых случаях больший эффект может дать, наоборот, комбинированная трансляция (часть значений параметра транслируется в один тип, часть — в другой, и т. п.).

Допустимо также использование нескольких маскирующих протоколов для обеспечения большей скрытности. При этом может использоваться статистика использования таких протоколов реальными людьми и, например, имитация деятельности человека. Например, исходный протокол может быть транслирован частично в HTTP, частично в SMTP, частично в протоколы мессенджеров — и для инструмента DPI он будет выглядеть как рядовой пользователь сети интернет.



Трансляция параметров протоколов

Прикладные аспекты

Немаловажным вопросом является способ задания схемы трансляции, по сути являющейся ключом, — ведь сторонам для успешного обмена необходимо обменяться ключами. Кроме ключей, необходимо также обменяться информацией о том, какой именно протокол выбран в качестве маскирующего.

Для описания ключа может быть использовано два подхода.

Первый подход заключается в том, чтобы явно, в табличном виде, описать, на какие параметры маскирующего протокола транслируются параметры исходного протокола. Достоинствами этого подхода является простота и возможность применения для протоколов, структура которых полностью неизвестна. Недостатком является громоздкость таблицы и, как следствие, сложность передачи такого ключа.

Второй подход использует не табличную схему трансляции, а алгоритмическую – выбор маскирующих параметров осуществляется, например, по определенной формуле. Такой подход более сложен в реализации, однако размер ключа при этом имеет существенно меньший объем.

Сама же процедура обмена ключами может использовать стандартные средства (например, использование защищенных каналов связи).

Заключение

Предложен способ обфускации (маскировки) одного прикладного протокола в другой. В некоторой степени данный подход похож на стеганографию, однако в последней акцент делается на встраивании информации в контейнеры (как правило, медиа-контейнеры), предложенный же подход обеспечивает именно трансляцию протокола «на лету».

Данный способ подходит для скрытого информационного обмена, где критичен сам факт обнаружения передачи данных. При использовании шифрования этот факт будет моментально установлен.

В открытых источниках не установлено факта применения такого подхода, что является преимуществом при реальном использовании.

Предметами дальнейших исследований являются следующие аспекты:

- Разработка конкретных методик и алгоритмов расчета величины delta;
- Анализ и выработка способов применимости технологии для бесконечных данных (например, бинарных);
- Разработка конкретной процедуры формирования схемы трансляции протоколов.

Литература

1. Windows Firewall Integration and Best Practices [электронный ресурс]. Режим доступа: https://docs.microsoft.com/ru-ru/previous-versions/windows/desktop/ics/windows-firewall-integration-and-best-practices (дата обращения: 03.10.2020).

2. Obfuscating a .NET Program: Worthwhile? [электронный ресурс]. Режим доступа: https://spin.atomicobject.com/2013/12/30/ obfuscation-dot-net/ (дата обращения: 05.05.2020).

3. Олифер В. Компьютерные сети. Принципы, технологии, протоколы / В. Олифер, Н. Олифер. – СпБ.: Издательский Дом ПИТЕР, 2005. – 462 с.

Network traffic obfuscation methods

A. O. Nevolin
Moscow Aviation Institute (National Research University), Moscow, Russia

Problems of hidden data transfer in nowadays communication network (Internet) are investigated. Method of veiled information transmission without encryption is proposed. Countermeasures against modern DPI tools are described.

Keywords: encryption, Tor, information security, veiled data transfer, network traffic obfuscation.

Bibliography — 3 references. *Received September 26, 2020*

Правила для авторов по оформлению рукописей статей, предлагаемых к публикации в журналах

Направляя рукопись статьи в редакцию журнала, авторы передают редколлегии и издателю журнала безвозмездное неисключительное право опубликовать ее на русском языке в качестве статьи в печатной и электронной версиях журнала в сети Интернет. При этом за авторами сохраняются их интеллектуальные права на рукопись статьи (в том числе "авторское право"). В связи с этим и с учетом Четвертой части (Раздел VII) Гражданского кодекса РФ авторами должно быть представлено в редакцию письмо в следующей форме:

Лицензионный договор о передаче права на публикацию
(издательский лицензионный договор)

Мы, нижеподписавшиеся, авторы рукописи ……., предоставляем редколлегии журнала и журнала и издателю ФГУП «НТЦ оборонного комплекса «Компас»

……..……
(название журнала)

безвозмездную простую (неисключительную) лицензию на публикацию рукописи статьи как в печатной, так и в электронной версиях журнала.

Мы подтверждаем, что данная публикация не нарушает интеллектуальных прав других лиц или организаций.

Подписи авторов: …… (ф.и.о., ученая степень, дата)

…….

…….

Статья должна быть подписана всеми авторами. В случае нескольких авторов указывается фамилия автора, ответственного за переписку с редакцией. Рукопись статьи направляется на адрес редакции журнала: 125424, Москва, Волоколамское ш., д. 77, ФГУП «НТЦ оборонного комплекса «Компас», Редакция журнала.

Дополнительная информация может быть получена в редакции при обращении по телефону: 8 (495) 491-43-17 или по E-mail: izdanie@ntckompas.ru.

Каждая статья рецензируется в соответствии с решением редколлегии журнала. Рецензенты выбираются из числа ученых и специалистов, компетентных в вопросах, рассматриваемых в статье, и имеющих собственные публикации в данном направлении. Решение о порядке публикации статьи принимается редколлегией с учетом мнения рецензентов. В случае разногласий среди членов редколлегии окончательное решение принимает главный редактор. При полном отклонении рукописи статьи от публикации редакция журнала направляет авторам мотивированный отказ. По этому факту редакция не вступает в полемику с авторами.

Комплектование статьи (обзора)

Статья должна быть представлена в редакцию в следующем комплекте:

- сопроводительное письмо, подписанное руководством организации;
- экспертное заключение о возможности опубликования в открытой печати и распространения в Российской Федерации и других государствах. При отсутствии в организации экспертной комиссии вместо экспертного заключения может быть представлено соответствующее заявление на имя главного редактора журнала от имени руководства организации, где работают авторы. В экспертном заключении или заявлении в обязательном порядке должна быть отражена возможность открытой публикации и передачи публикуемых материалов за границу.
- лицензионный договор по приведенному образцу;
- рукопись статьи — объем статьи (без рисунков) не должен превышать 10 страниц формата А4 при 1,5 межстрочных интервалах, а объем статьи обзорного характера — 20 страниц. Рекомендуемая гарнитура — New Times Roman. Размер шрифта — 12;
- Материал статьи представляется в редакцию в печатном виде (на бумажном носителе) и в электронном варианте на CD/DVD-диске с текстом в формате Word.

Оформление статьи:

- статья начинается с указания УДК;
- название статьи набирается строчными буквами (кроме начальной прописной) полужирным шрифтом, размер шрифта 14, для остального текста используется простой шрифт размером 12, причем рекомендуемая гарнитура шрифта — Times New Roman;

- после названия — список авторов, инициалы авторов предшествуют их фамилиям;
- с отступлением в 2 строки представляется аннотация статьи;
- далее приводится список ключевых слов для данной статьи (не более десяти);
- страницы текста нумеруются без пропусков и добавлений литерных обозначений (типа 1*а*, 2*б* и т. п.), причем в сквозную нумерацию должны быть включены все элементы статьи;
- внизу первой страницы текста помещается отдельный абзац (с полужирным шрифтом), содержащий контактную информацию об авторе (или авторах) в следующем виде: фамилия, имя, отчество, должность, ученая степень, почтовый адрес предприятия, телефон, E-mail;
- основной текст статьи должен начинаться с четкой постановкой цели и задач работы, сопровождаемой аргументами в пользу ее выполнения на фоне существующего состояния затронутой в статье проблемы. Дальнейший текст статьи также должен иметь смысловые рубрикаторы (разделы и подразделы) без их нумерации. Заканчиваться статья должна отдельным разделом «Заключение» с перечислением основных результатов, следую-щих из них выводов и, по возможности, предложений по развитию исследований и использованию их результатов.
- после основного текста — список использованных источников "Литература" (не менее 5 источников); Список использованной литературы должен соответствовать всем ссылкам на внешние источники в тексте статьи. Ссылки оформляются в квадратных скобках, например, [1—6], [7, 8]. Внутренние ссылки, т. е. ссылки на формулы, рисунки и таблицы статьи оформляются с использованием круглых скобок, например, формула (1), уравнение (4), (рис. 3), (табл. 2). Любые ссылки в подписях к рисункам и в самих рисунках не рекомендуются;
- далее размещается подробная англоязычная информация о статье: название статьи, фамилия и инициалы авторов (английская транслитерация), предприятие, аннотация, ключевые слова (Keywords).

Оформление рисунков:

- рисунки и графики вставляются непосредственно в нужном месте в статье и в желаемом масштабе.
- рядом с осями графиков указываются отображаемые физические величины только в символьной (буквенной) форме, а через запятую — размерность величины по-русски (прямым шрифтом). Различные кривые на графиках рекомендуется нумеровать, даже если они характеризуются отдельным цветом или типом линии. Графики представляются только на белом фоне. Вспомогательные сетки на площади графика не допускаются;
- подписи под соответствующими рисунками (полужирный курсивный) представляются в нужных местах текста. Каждая подпись должна быть по возможности лаконичной, но емкой по содержанию.

Оформление формул:

- простые формулы вводить в текст в формате используемого текстового редактора, более сложные формулы — с использованием редактора формул MathType;
- стандартные математические обозначения (например, max, log, sin, exp и т. д.) должны быть набраны прямо. То же относится к цифрам и числам;
- для символьного обозначения невекторных физических (технических) величин использовать только латинский и греческий алфавиты, при этом в тексте для греческих букв использовать прямой шрифт, для латинских букв — наклонный шрифт (курсив);
- векторы и матрицы обозначать полужирным прямым шрифтом;
- для нижних и верхних индексов применять арабские цифры, латинские или греческие буквы. Если индекс представляет собой сокращенную форму русского слова — характеристики, то допустимо использовать в его обозначении русские буквы (прямой шрифт), например $U_{вх}$, $I_{вых}$, $v_{гр}$ и т. п.
- размерность физических величин обозначается всегда только по-русски прямым шрифтом.

Оформление таблицы:

- содержание таблицы не должно дублировать данные, приводимые на графиках или в тексте;
- графы должны иметь название без сокращения отдельных слов.

Рисунки, формулы и таблицы должны иметь свою отдельную сквозную нумерацию. Если на конкретную формулу нет дополнительных (возвратных) ссылок в тексте или она в единственном числе, то нумерация ее не нужна. Единственные таблица и/или рисунок также не нумеруются.

При публикации в журнале каждая статья (в контактной информации) сопровождается сноской со знаком охраны авторского права ©, поставленным перед фамилией автора (фамилиями авторов) и годом издания.

Авторы (или автор) каждой статьи после выхода журнала в свет имеют право на получение от редакции электронной версии статьи в PDF-формате (редактор Adobe Acrobat).