ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

1
(132)

Подписывайтесь,
читайте,
пишите в наш журнал

Москва 2021

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

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

1 (132)

Москва 2021
Основан в 1974 г.

СОДЕРЖАНИЕ

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2021. Вып. 1 (132). С. 1—48.

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

Подписано в печать 24.03.2021.
Формат 60×84 1/8. Бумага офсетная.
Усл. печ. л. 5,8. Уч.-изд. л. 6,0.
Тираж 400 экз. Заказ 1969.
Свободная цена.
Адрес редакции: 125424, Москва,
Волоколамское ш., 77.
ФГУП «НТЦ оборонного комплекса «Компас».
http://ntckompas.ru
Отпечатано: 101000, Москва,
Лубянский проезд, д. 15, стр. 4, офис 105.
ИП Кириченко Алексей Викторович.
Индекс 79187.

УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004.457
DOI: 10.52190/2073-2600_2021_1_3

Анализ средств обратного проектирования сетевых протоколов

В. С. Джум; В. А. Лосев
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Проведён анализ и рассмотрено актуальное программное обеспечение для анализа сетевых протоколов и выполнения их обратного проектирования, которым может воспользоваться разработчик в процессе своей деятельности.

Ключевые слова: модель взаимодействия открытых систем, обратное проектирование сетевого протокола, сетевой след.

Обратное проектирование сетевых протоколов используют во многих аспектах информационной безопасности, например для извлечения спецификаций и описания закрытого протокола. Так, сетевые фильтры, которые исследуют трафик приложения, должны знать спецификацию протокола, чтобы эффективно защищать пользователя от потенциальных угроз. Чаще всего они анализируют уже протоколы 7-го уровня модели взаимодействия открытых систем (BOC, OSI). Таким образом, обратное проектирование протоколов является ключевым аспектом в разработке таких устройств и продуктов, чтобы они могли эффективно работать с большим количеством протоколов.

Помимо этого предварительная информация о спецификации протокола очень полезна для оценки полноты (с точки зрения базы протоколов, которые поддаются анализу разрабатываемым приложением) и надёжности (с точки зрения устойчивости приложения к тестам разного характера) разрабатываемого приложения для обеспечения безопасности. Для того чтобы провести подобное оценивание, аудитору необходимо создать реалистичный поток данных, который содержит как правильные пакеты протокола, так и пакеты с различными отклонениями или вовсе неизвестные для приложения. Отсюда следует, что устройство, которое используют для создания подобного трафика, должно обладать полной спецификацией для точного воссоздания протокола. Например, инструменты анализа уязвимостей и фаззинга могут использовать спецификации протокола, чтобы создать недопустимые и/или неожиданные данные в полях сообщения (например, переполнение буфера, неправильные переходы между состояниями и т. д.), которое затем отправляется клиенту. Данный подход носит название "умный фаззинг". Он требует полного понимания как формата сообщений, так и автомата протокола (протокольного языка), чтобы получить правдивые результаты. Формат сообщений включает в себя тип пакета и их структуру. Протокольный язык (грамматика протокола) — это набор правил, описывающих обмен сообщений из последовательности пакетов.

Джум Владимир Сергеевич, ассистент кафедры "Радиосистемы и комплексы управления, передачи информации и информационная безопасность".
E-mail: dghum1996@mail.ru
Лосев Владислав Алексеевич, аспирант кафедры "Радиосистемы и комплексы управления, передачи информации и информационная безопасность".
E-mail: 2075100@mail.ru

Статья поступила в редакцию 21 декабря 2020 г.

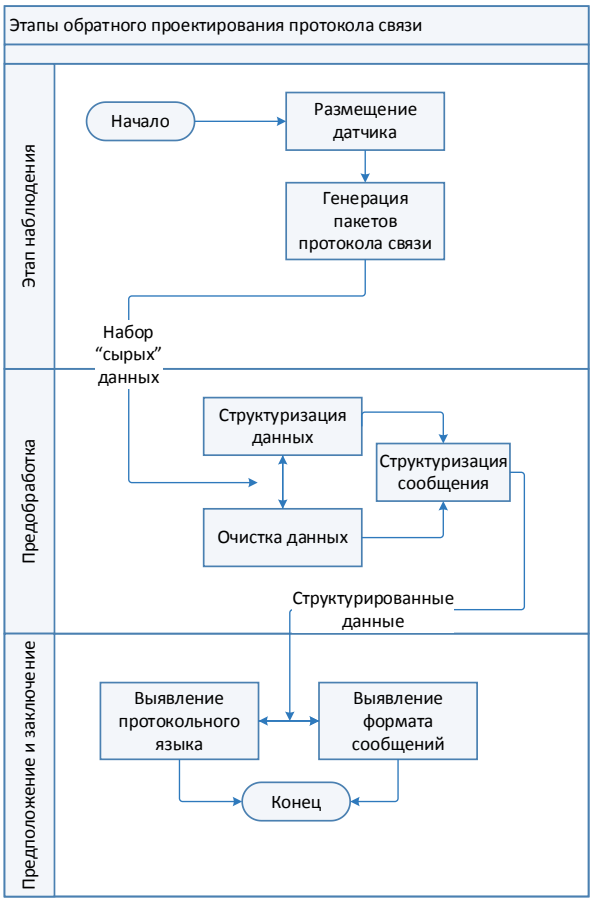
Обратное проектирование сетевых протоколов также очень высоко ценится в среде противостояния вредоносному программному обеспечению. Например, чтобы выявить утечку информации и сторонние контроллеры (сервер бот-сети и т. п.), а также в целях обезвреживания последнего без обнаружения, аналитики вредоносных программ должны понимать внутреннее устройство и поведение протокола.

Таким образом, для создания пакетов, аудита полноты и надёжности продуктов сетевой безопасности и анализа вредоносных программ необходимо выяснить спецификацию неизвестного или изменённого протокола. Однако данный процесс является очень ресурсоёмким, его не всегда может выполнить человек, неспособный обработать сотни тысяч сетевых пакетов, которые генерируют современные операционные системы. Использование таких утилит, как Wireshark, для фильтрации пакетов также не всегда удобно, поскольку неизвестные протоколы могут пользоваться стандартными портами или вовсе маскироваться под уже существующие протоколы. Кроме того, зависимость между полями пакетов может быть как линейной, так и нелинейной. Сам размер полей может меняться, как и само наличие этих полей. В связи с этим когда перед разработчиком встаёт необходимость провести подобный анализ, он может либо написать своё решение, либо воспользоваться уже существующими разработками, автоматизирующими этот процесс, и выяснить, подходят ли они ему.

В данной работе будут представлены существующие решения и описание каждого из них для понимания текущего состояния средств для обратного проектирования сетевых протоколов.

Этапы обратного проектирования протокола информационного взаимодействия

Обратное проектирование протокола информационного взаимодействия состоит из следующих этапов (рисунок).



Этапы обратного проектирования протокола связи

Предварительный этап обратного проектирования протокола нацелен на идентификацию и описание характеристик окружения. На основе данных сведений специалист может приступить к этапу наблюдения, который заключается в установке необходимого программного и/или аппаратного обеспечения (оборудования), нацеленного на сбор сетевых пакетов. Следующий этап состоит в обработке полученных данных, их очистке от посторонних данных и выявлении требуемого набора пакетов. Последним этапом является выявление структуры сообщений или языка протокола из сообщений, полученных на прошлом этапе.

Эти шаги выполняют последовательно. Обычно они в значительной степени зависят от опыта и интуиции специалиста, проводящего анализ. Успех структуризации и исследования протокола значительно зависит от того, насколько хорошо специалист может проследить закономерности, и от эффективности средств, которые он использовал для автоматизации анализа.

Этап наблюдения. Вывод обратного проектирования основан на сборе следов, полученных благодаря наблюдению за каналом связи. На данном этапе есть две проблемы. Размещение датчика обязательно для перехвата данных в рамках процесса обратного проектирования протокола. Для исследования протоколов размещение датчиков может представлять значительную проблему в том случае, когда приложение использует несколько протоколов для взаимодействия, и все протоколы располагаются в разных каналах. Таким образом, необходимо идентифицировать соответствующие каналы. Более того, если протокол использует разные каналы, то для каждого из каналов потребуется свой датчик. Неправильное размещение датчиков может привести к неполным данным и, соответственно, к неполному анализу. Серьёзное испытание представляет размещение датчика в случае, когда протокол связи использует шифрование. Например, может потребоваться размещение датчиков внутри устройства передачи и/или приёма. Одно из решений заключается в установке датчика сразу после процедуры дешифрования на принимающем устройстве.

Этап предобработки. Предобработка заключается в сборе следов. В зависимости от правильности расположения датчиков на предыдущем этапе указанный этап может представлять собой нетривиальную задачу. Прежде всего, кроме искомого протокола, в канале связи может присутствовать значительное количество побочных пакетов, т. е. пакетов других протоколов, которые необходимо отфильтровать. Помимо этого данные протокола могут быть:

- вложены в другой протокол;
- разделены на несколько протоколов;
- быть скрыты среди большого количества побочных пакетов.

Таким образом, первая проблема на рассматриваемом этапе — корректно обработать данные, убрав все побочные, т.е. произвести очистку собранных данных.

Если сообщение отправляется несколькими пакетами данных, это добавляет ещё одну проблему: анализ и сборку нескольких пакетов, а также их отслеживание для реконструкции подходящего для анализа сообщения. Для сетевых протоколов, например, когда происходит анализ протокола на основе технических средств реабилитации (TCP), необходимо собрать несколько TCP сегментов, чтобы получить информацию про сообщение уровня приложений (7-го уровня модели OSI). Также сетевые пакеты могут содержать сразу несколько сообщений. Следовательно, их необходимо разделить. Обе операции являются частью процесса структуризации данных.

После реконструкции соответствующих сообщений их необходимо сгруппировать в классы сообщений, что также относится к задачам структуризации данных. Эта стадия необходима для сравнения сообщений, которые имеют семантическую схожесть, она состоит в нахождении функции, которая позволит идентифицировать тип сообщения исходя из последовательности байтов, а также предоставит степень расхождения данного сообщения с другими схожими.

Этап предположения и заключения. Процесс выявления формата сообщения направлен на идентификацию пакетов одного типа и их структуры, а процесс выявления протокольного языка (грамматики) нацелен на ре-

конструкцию правил, описывающих обмен сообщений из последовательности пакетов.

В обоих случаях важно определить зависимость между разными полями сообщения или между сообщениями. Конечной целью обратного проектирования протокола является получение спецификации для формата сообщения или протокольной грамматики. Подобная спецификация отображается в виде модели. При этом необходимо выбрать достаточно подробную модель протокола, чтобы она могла полностью отобразить исходную спецификацию. Например, некоторые сложные форматы сообщений или протокольной грамматики могут иметь вид дерева или даже рекурсивный вид. Такие структуры означают, что сообщение или значение поля зависит от других значений в сообщении или сообщениях. Таким образом, построение грамотной модели представляет большую сложность. Неправильный выбор может привести к спецификации, которую невозможно использовать для всего спектра сообщений, применяемых в изначальном протоколе.

Проблемы в процессе обработки сетевых следов

Протокол связи определяется правилами, которые позволяют одному или множеству объектов (или субъектов) взаимодействовать друг с другом. Иными словами, это язык, который они используют для общения между собой [1]. Как уже упоминалось, спецификация протокола, как и большинства языков, состоит в основном из:

- словаря, т. е. набора сообщений и формата этих сообщений;
- грамматики, определяющей процедурные правила, которые представляют допустимые последовательности сообщений, обычно моделируемые как конечные автоматы.

Впоследствии для создания сообщений протокола необходимо понимание и словаря, и грамматики. Рассмотрим только первый аспект — словарь. Работы по обратному проектированию форматов сообщений делят на две группы в зависимости от подхода, анализируют они реализацию протокола на уровне компьютерного приложения [2] или сетевые следы на уровне сети [3]. Первый подход предполагает выявление формата сообщений с помощью наблюдения за конкретной реализацией протокола для рассмотрения процесса синтаксического анализа и генерации сообщений в данной реализации протокола. Для этого требуется отладка программной реализации. К сожалению, данный подход сложен в автоматизации в силу индивидуальности программной реализации. Сложности могут возникать из-за разных методов противодействия анализу программной реализации. К ним относятся:

- обфускация;
- сжатие кода;
- антиотладка.

В связи с этим в данной работе внимание сконцентрировано только на приложениях, которые анализируют сетевые пакеты, т. е. на основе сетевых следов.

Закрытые протоколы (проприетарные) и более специфичные протоколы, которые используются вредоносным программным обеспечением, могут использовать шифрование для защиты процесса обмена сообщениями. Такие механизмы могут значительно ограничить возможности алгоритма анализа сетевых следов протокола. Существуют решения, которые позволяют обходить данное ограничение. Они используют методы анализа оперативной памяти устройства и пытаются извлечь данные до процесса шифрования [4]. Однако даже с учетом доступа к протоколу возникает вопрос о том, как после вскрытия протокола эмулировать его. Эта проблема бывает особо острой, если в протоколе используется нестандартное шифрование. В связи с этим автоматизация данного процесса очень сложна и близка к невозможной, поэтому не будем рассматривать протоколы, использующие шифрование.

Как уже упомянуто ранее, распознавание формата сообщения обычно происходит в два основных этапа: создание массивов схожих сообщений и разделение полей внутри сообщений. Сбор массивов сообщений происходит с помощью разделения сообщения на токены с использованием *n*-граммы, разделителей или алгоритмов выравнивания последовательностей. Затем выполняется создание массивов синтаксически схожих сообщений на основе сравнения типа (бинарный или ASCII) и/или значений каждого из токенов. Массивы сооб-

щений создают на основе результата сравнения сообщений между собой в целях выявления схожих сообщений. Следующим шагом является распознавание полей внутри самого сообщения. Это осуществляют путем нахождения статических и динамических полей в массиве сообщений и повторяющихся разделителей, если они есть.

Средства обратного проектирования сетевых протоколов

Рассмотрим программные средства, которые нацелены на анализ сетевого трафика и помощь в обратном проектировании. Данные средства поделены на две категории. Первая категория анализирует только формат сообщений, вторая — старается предоставить данные обо всей грамматике протокола. В таблице приведены все рассматриваемые приложения в хронологическом порядке их создания. Следует отметить, что значительная часть средств ориентирована на анализ формата сообщений, который является предварительным шагом для анализа грамматики протокола.

Средства анализа сетевого протокола

Год создания	Анализ формата сообщения	Анализ грамматики протокола
2004	PI Project	—
2005	ScriptGen	ScriptGen
2006	RolePlayer	—
2007	Discoverer	—
2010	ASAP	Veritas
2011	ReverX Netzob	ReverX Veritas
2012	Netzob	Netzob PRISMA
2014	Netzob	Netzob

Первое рассматриваемое средство, PI Project [5, 6], использует алгоритмы биоинформатики для анализа формата сообщений. При этом оно не занимается протокольной грамматикой. Данное средство использует алгоритм Нидлмана—Вунша, чтобы соотнести последовательность байтов у пары сообщений. Оптимальное соотнесение позволяет идентифицировать схожие части двух сообщений, которые отвечают за одни поля. Этот результат будет использован для построения иерархического дерева, которое описывает иерархическую классификацию сообщений на основе их степени схожести (основная часть схожих сообщений расположена в соседних ячейках в дереве). Для данной цели применяют алгоритм UPGMA. При этом пользователю необходимо вручную разделить дерево, чтобы идентифицировать классы сообщений. Указанную идею разработки в дальнейшем использовала значительная часть других средств анализа сетевых пакетов.

Вскоре появилось средство, называемое ScriptGen [6, 7]. Оно способно создавать набор скриптов, которые эмулируют сетевой протокол, установленный на сервере, для honeypot, используемого в атаке Honeyd. Таким образом, Scriptgen в отличие от PI project требует проведения анализа грамматики протокола. Он начинается с этапа предварительной обработки, который состоит из следующих фаз:

- фильтрация незначимых пакетов и сохранение пакетов, которые соответствуют интересующему протоколу;
- воссоздание сообщений протокола из этих пакетов.

Разделение сообщений на классы выполняется автоматически с учётом порогового значения. Заключение о грамматике протокола основано на регулярном языке. Результирующая модель — это детерминированный конечный автомат, содержащий наиболее часто используемые ответы, которые возвращает сервер.

В тот же период был представлен Roleplayer, который настроен на повторное воспроизведение сообщений в других условиях, в частности при изучении деталей сценария атаки на сеть. Повторное воспроизведение сообщений включает в себя адаптацию сетевых следов для определения характеристик окружения (изменение IP-адресов, номера TCP-пакета и т. д.). Данная операция требует точного знания полей сообщений, их соответствия окружению и их зависимости.

Чтобы получить эти данные, Roleplayer использует подход активного анализа, во время которого обмен сообщениями имитируется

средством для идентификации соответствий. Дополнительно, используя алгоритм соотнесения, средство может обучиться находить определенные зависимости между полями сообщения (например, размер и значения куки-файлов и т. д.). Однако поля, вложенные в другие поля, не могут быть корректно распознаны. Чтобы справиться с этой сложностью, использован новый подход в средстве Discoverer. Вместо использования алгоритма Нидлмана—Вунша предполагают, что разделители полей сообщения известны (пробел, перенос строки/возврат каретки, табуляция, точка с запятой и т. д.), что значительно упрощает решение данной проблемы. После разделения полей сообщений средство применяет к полям сообщения иерархическую и рекурсивную классификацию, что позволяет идентифицировать вложенные значения. Наконец, используется набор эвристических алгоритмов для идентификации зависимости между полями.

В то время как значительная часть исследований и средств, которые используют для обратного проектирования протоколов, нацелена на анализ формата сообщений, Vertitas [8, 9] нацелен на анализ грамматики протокола. Для выполнения данной задачи требуется только тип сообщений без какой-либо информации об их формате. Типы сообщений распознают на основе наиболее часто используемой последовательности байтов, наблюдаемой в заголовке пакета (первые *n* байтов). Предполагают, что заголовок сообщения расположен в начале сообщения и содержит особый набор байтов, который описывает класс сообщения. Указанное предположение позволяет значительно снизить количество данных, необходимых для обработки. Следом за этим этапом идёт непосредственно сам анализ грамматики протокола. Разработчики используют предположение, что сообщения отправляются только в зависимости от последнего отправленного сообщения, а не от всей истории обмена сообщениями. Модель, построенная этим инструментом, является автоматом, в котором содержатся классы сообщений и вероятности получения такого сообщения. Порог служит для удаления сообщений, которые редко применяют. Следует отметить, что используя подобную логику, данное средство отрезает последовательности сообщений, которые соответствуют необычному событию или поведению сервера. В таком случае полученная грамматика частична и не содержит все возможные события, которые наблюдались при обмене сообщениями.

ASAP [10] также больше нацелен на классификацию сообщений, чем на повторение точного формата обмена сообщениями. Он разработан для улучшения анализа, которому подвергаются вирусы и данные, собранные из honeypots, и для помощи проектированию системы обнаружения вторжений. Из наблюдаемых сообщений выделяют базовые идентификаторы: на основе заранее определённых разделителей в случае с текстовыми сообщениями или фиксированного значения размера идентификатора в случае с бинарными. Это приводит к построению алфавита, используемого для характеристики полезной нагрузки сети, которая отображается в векторном пространстве. Шаблон общения сопоставляют с основными направлениями в векторном пространстве, а затем идентифицируют. Эти заготовки позволяют получить представление о базовом взаимодействии систем. Помимо особенных техник, используемых для определения базовых признаков, основное отличие ASAP от других средств состоит в применении математического подхода. Однако выявленный формат сообщений является не совсем точным. Также средство не показывает возможные взаимосвязи между обнаруженными идентификаторами и порядок их возникновения.

Позже разработчики ASAP расширили его, добавив новые возможности. Была добавлена возможность анализа протокольной грамматики, связанной с полезной нагрузкой сетевого пакета. Это привело к разработке PRISMA [11]. Данное средство использует такую же стратегию, что и ASAP, однако математический анализ в нем заменён классификацией сообщений на основе метрик (расстояний). Инструмент строит скрытую цепь Маркова на основе наблюдаемой последовательности типов сообщений. Эта модель хорошо подходит для определения изменений в состоянии протокола, которые необязательно приводят к отправке сообщений.

ReverX использует одинаковый подход к анализу формата сообщений и протокольной грамматики. Данное средство делит сообщения на поля с помощью заданного набора разделителей. Затем создаётся цикличный аппарат для моделирования возможных последовательностей полей. Циклы помогают в генерации модели и включают ненаблюдаемые сообщения. Такие автоматы моделируют формат сообщений. Схожий процесс используется для создания протокольной грамматики из наблюдаемой последовательности типов сообщений. У данного приложения есть несколько интересных функций, в частности относительно возможности обобщения формата сообщений, что представляет значительную проблему при обратном проектировании протоколов. Однако этот метод, используемый для разделения сообщений по полям, не подходит для бинарных сообщений.

Еще одним подходящим средством является Netzob [12], которое служит предметом множества исследований, развивающихся в течение последних нескольких лет. Изначально оно было разработано для оказания помощи в моделировании ботнет-сетей. Авторы использовали вариант автомата Мили для моделирования грамматики протокола путем добавления информации о времени, прошедшем между двумя наблюдаемыми сообщениями. Такую грамматику изучают с помощью активного подхода, основанного на алгоритме L^*. Далее автоматы делают недетерминированными, добавляя вероятность отправки сообщения с учетом состояния и полученного сообщения. В качестве алгоритма анализа сообщений и их классификации используют алгоритм Нидлмана—Вунша. Авторы используют специальный эвристический алгоритм для локального соотнесения двух сообщений, не принимая во внимание все содержание сообщений. Кроме того, проводится анализ семантики сообщений. При этом различные уже проанализированные атрибуты сохраняются в виде сообщений, так как эта информация может помочь при уточнении результатов анализа. Для анализа грамматики протокола используют активный подход, в то время как пассивный используется для анализа формата сообщений. Также с помощью активного подхода можно добиться определенных улучшений в анализе формата сообщений. Кроме того, могут использоваться временные соотношения для взаимосвязи сообщений и действий протоколов. С одной стороны, это позволяет идентифицировать поля сообщений с изменяемым содержимым, а с другой — соотносить семантику с каждым классом сообщения. Однако такой подход подразумевает дополнительные усилия специалистов, которые не всегда можно автоматизировать. Для значительного уменьшения времени обучения автомата Мили можно использовать метод, подразумевающий разделение основного автомата на части, связанные действиями, выполняемыми системой. Важно отметить, что Netzob имеет расширения для вывода результатов работы в различных форматах, подходящих в том числе для фаззинга и симуляции работы систем передачи данных.

Применение средств обратного проектирования

В данной статье рассмотрены этапы, необходимые для обратного проектирования сетевого протокола. Приведен сравнительный анализ существующих решений. Разработчики продуктов, обеспечивающих безопасность сети с применением анализа протоколов 7-го уровня, могут использовать автоматические средства анализа, так как они позволяют добиться достаточно высокой точности в условиях полной автоматизации. То же самое касается специалистов, работающих с выявлением вредоносного программного обеспечения. Подобное автоматизированное программное обеспечение по обратному проектированию сетевых протоколов может значительно увеличить скорость их реакции на появление нового типа бот-сетей.

Выводы

Количество средств, используемых для обратного проектирования и открытых для публики, ограничено. Многие антивирусные компании используют свои личные наработки для анализа вредителей или полагаются на полуручной труд аналитиков.

Стоит отметить, что правовая основа для обратного проектирования уже существует в гражданском кодексе Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ. Помимо этого в 2016 г. на заседании Правительственной комиссии по импортозамещению министр промышленности торговли РФ Д. В. Мантуров заявил о планах создания на базе Фонда развития промышленности центра обратного инжиниринга.

Всё это служит стимулом к усовершенствованию методов обратного проектирования с использованием его на благо государства. Данный анализ является первым этапом на этом пути.

Литература

1. *Holzmann G. J.* Design and validation of computer protocols. — Prentice-Hall, Inc., 1991.
2. *Caballero J., Poosankam P., Kreibich C., Song D.* Dispatcher: enabling active botnet infiltration using automatic protocol reverse-engineering. In Proceedings of CCS, 2009.
3. *Beddoe M. A.* Network protocol analysis using bioinformatics algorithms. — In Toorcon, 2004.
4. *Leder F., Martini P.* Ngbpa next generation botnet protocol analysis: Emerging Challenges for Security, Privacy and Trust, V. 297 of IFIP Advances in Information and Communication Technology. — Berlin-Heidelberg: Springer, 2009.
5. Network Protocol Analysis using Bioinformatics Algorithms [Электронный ресурс]. URL: http://www.4tphi.net/~awalters/PI/pi.pdf (дата обращения: 18.07.2020).
6. *Caballero Bayerri J.* Grammar and model extraction for security applications using dynamic program binary analysis. Ph. D. thesis, Carnegie Mellon University, 2010.
7. *Leita C., Mermoud K., Dacier M.* ScriptGen: an automated script generation tool for Honeyd: Computer Security Applications Conference, 21st Annual, 2005. P. 12.
8. *Wang Y., Zhang Z., Guo L.* Inferring Protocol State Machine from Real-World Trace. Recent Advances in Intrusion Detection. № 6307. Lecture Notes in Computer Science. 2010. P. 498—499.
9. *Wang Y., Zhang Z., Yao D. D., Qu B., Guo L.* Inferring Protocol State Machine from Network Traces: A Probabilistic Approach // Applied Cryptography and Network Security. № 6715. Lecture Notes in Computer Science. 2011. P. 1—18.
10. *Krueger T., Krmer N., Rieck K.* ASAP: Automatic Semantics-Aware Analysis of Network Payloads // Privacy and Security Issues in Data Mining and Machine Learning. № 6549. Lecture Notes in Computer Science. 2010. P. 50—63.
11. *Krueger T., Gascon H., Krmer N., Rieck K.* Learning Stateful Models for Network Honeypots // Proceedings of the 5th ACM Workshop on Security and Artificial Intelligence, AISec '12, 2012. P. 37—48. http://doi.acm.org/10.1145/2381896.2381904.
12. *Bohlin T., Jonsson B.* Regular Inference for Communication Protocol Entities // Technbical Report. 2008. № 024.

Analysis of network protocol reverse engineering tools

V. S. Dzhum, V. A. Losev
Moscow Aviation Institute (National Research University), Moscow, Russia

This article analyzes and considers current software for analyzing protocols and performing their reverse engineering, which a developer can use in the course of his activities.

Keywords: open systems interconnection model, network protocol reverse engineering, network trace.

Bibliography 12 references. *Received December 21, 2020*

ДОВЕРЕННАЯ СРЕДА

УДК 004

DOI: 10.52190/2073-2600_2021_1_11

Применение подходов и средств создания доверенного сеанса связи для безопасной работы гипервизоров в системах виртуализации

А. Д. Хмельков
ОКБ САПР, Москва, Россия

Рассмотрены методы защиты гипервизоров от несанкционированного внесения изменений в образ. Предложен новый метод защиты.

Ключевые слова: гипервизоры, ESXi, несанкционированный доступ, доверенная загрузка, доверенный сеанс связи.

Технологии виртуализации приобретают всё большую популярность. Это подтверждается как личными наблюдениями автора, так и результатами исследований (см. например, [1—3]). Виртуализация позволяет использовать ресурсы одной и той же физической ЭВМ различным пользователям с сохранением изоляции виртуальных машин различных пользователей и с возможностью использования удалённого доступа к ресурсам ЭВМ. Для обеспечения управления виртуальными машинами на физической ЭВМ (назовём её сервером) необходим гипервизор — программное или программно-аппаратное средство, устанавливаемое на сервер и предоставляющее доступ к его ресурсам.

Цель работы — рассмотреть методы защиты гипервизоров от несанкционированного доступа (НСД), провести обзор существующих решений, а также предложить новый метод на основе создания доверенного сеанса связи (ДСС). Актуальность темы заключается в том, что развитие технологий виртуализации ведёт к увеличению количества атак на эти системы, а существующие решения обладают рядом недостатков. Новизна работы состоит в том, что в ней предложено решение, в котором гипервизор расположен на защищённом от записи разделе внешнего носителя, что автоматически гарантирует его целостность при загрузке.

Хмельков Алексей Дмитриевич, программист.
E-mail: a.hmelkov@okbsapr.ru

Статья поступила в редакцию 11 декабря 2020 г.

Материалы и методы

Для решения поставленных задач сначала подробнее опишем объект исследования — гипервизоры, затем проведём обзор существующих решений, опишем их недостатки и далее предложим новое решение, для которого не будут характерны недостатки уже имеющиеся.

Гипервизоры бывают двух типов: устанавливаемые непосредственно на "железо" сервера и не требующие для своей работы операционной системы, а также те, которым для взаимодействия с "железом" требуется операционная система. В данной статье мы будем рассматривать гипервизоры первого типа. Защита гипервизоров второго типа сводится главным образом к доверенной загрузке ОС, посредством которой они взаимодействуют с "железом".

По статистике к наиболее популярным гипервизорам, устанавливаемым непосредственно на "железо", относятся VMWare ESXi (далее ESXi), Hyper-V и KVM [4].

Подробнее рассмотрим решение на базе гипервизора ESXi, хотя оно также может быть реализовано на базе любого другого из пере-

численных гипервизоров. Структура разделов ESXi выглядит следующим образом: EFI-раздел, два boot-bank (основной и резервный). При переходе с версии ESXi 6 на ESXi 7 неиспользуемые для загрузки остальные разделы объединены в один, хранящийся в долговременной памяти. Структура разделов в версиях 6 и 7 представлена на рис. 1. Более подробно о структуре ESXi можно прочитать в документации [5].

Объект защиты представляет собой находящийся внутри контролируемой зоны сервер, на котором должен функционировать гипервизор ESXi. На сервере расположены защищённые (например, при помощи Аккорда-В) виртуальные машины, к которым через сеть могут подключаться клиенты. Защита клиентов и защита сети выходят за рамки исследования, так как непосредственно к защите гипервизоров не относятся, поэтому в настоящей работе рассмотрены не будут. Схема объекта показана на рис. 2. Тёмным цветом выделена область, защита которой рассматривается в данной статье.

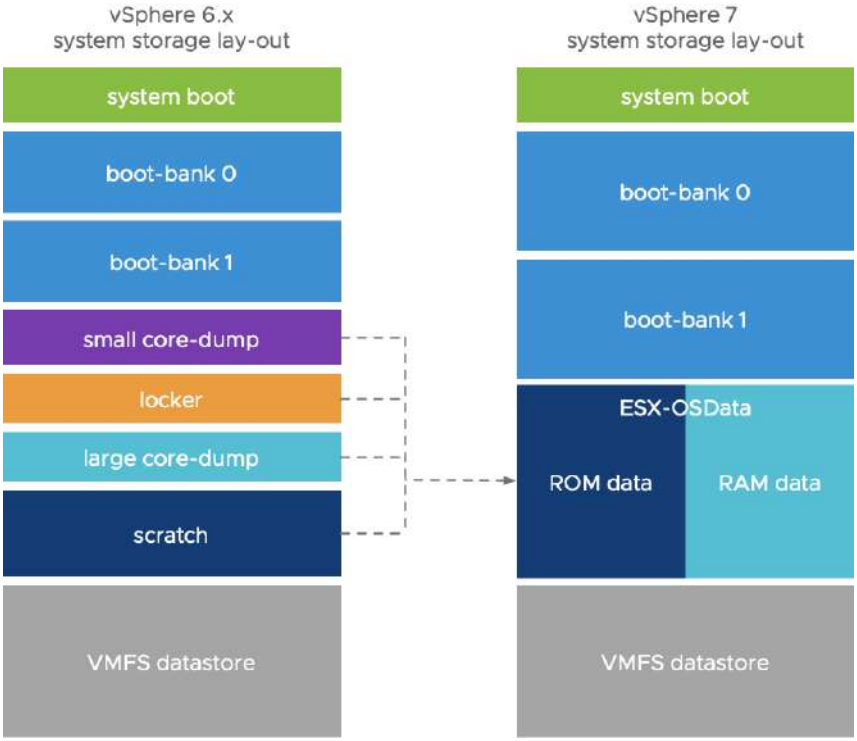


Рис. 1. Структура разделов ESXi в версиях 6 и 7

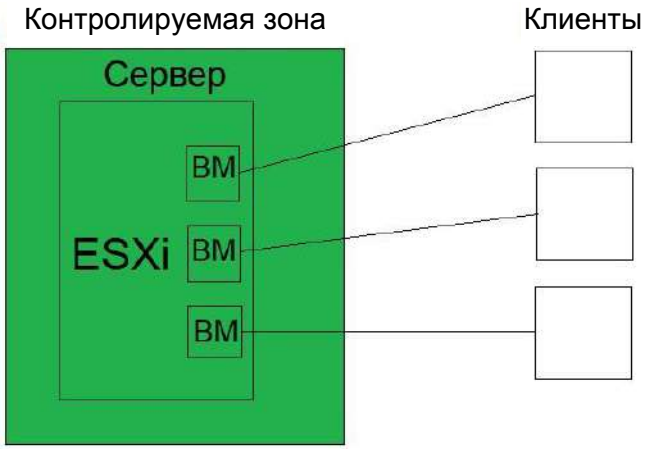


Рис. 2. Схема объекта

Для гипервизоров характерно наличие угрозы НСД, точнее одной из разновидностей НСД — несанкционированного внесения изменений в образ гипервизора, в результате которого может быть нарушена целостность программного обеспечения (например, установлено вредоносное ПО). Нарушение работы гипервизора может привести к нарушениям работы сервера, что, в свою очередь, может повлечь нежелательные последствия и на клиентских ЭВМ (например, возможны отказ в обслуживании или распространение вредоносного ПО).

Обзор литературы

Существует несколько подходов по обеспечению защиты гипервизора от НСД. Один из них — использование средств доверенной загрузки (СДЗ), таких, как Аккорд-АМДЗ, о котором подробнее можно прочитать в [6], Инаф, Средства доверенной загрузки (СДЗ) уровня BIOS. Данный метод надёжен, но имеет ряд недостатков. Для использования Аккорда-АМДЗ необходимо наличие свободного слота PCI-express, который имеется не на всех современных серверах. Для подключения Инаф необходим свободный USB-порт, которых может быть мало. Кроме того, USB-порт необходим для подключения аппаратного идентификатора, работающего с СДЗ. СДЗ уровня BIOS не требует ни слота PCI-express, ни USB-порта (кроме как для идентификатора), но в некоторых серверах BIOS защищён от записи программными средствами, а использование программатора может быть затруднено, если чип с BIOS не является съёмным.

Альтернативный подход к обеспечению защиты гипервизора от НСД — использование средства обеспечения доверенного сеанса связи (подробнее о концепции которого см. в [7, 8]). Это устройство представляет собой загрузочную флэшку с несколькими разделами, для каждого из которых установлены свои политики чтения и записи, способные меняться при вводе корректного пин-кода [9]. ESXi можно разместить на разделе с правами Read only, с которого и будет производиться загрузка. В результате будет решена проблема целостности объектов гипервизора, т. е. не надо будет дополнительно проверять целостность компонентов гипервизора, а сам носитель, если его выставить первым загрузочным устройством в настройках BIOS сервера, будет выполнять функции перехвата управления. Таким образом, получится своего рода "неатомарный" РКБ, описанный в [10]. Проблема размещения ESXi на неизменяемом разделе — невозможность обновления, которое периодически требуется для гипервизора. Решением данной проблемы может стать временный перевод раздела с ESXi в режим Read-Write (RW).

Результаты

Рассмотренные решения обладают рядом недостатков. Далее опишем устройство, для которого эти недостатки не будут характерны. Устройство представляет собой защищённый загрузочный носитель. На носителе с установленным специальным ПО, позволяющим разграничить доступ к разделам носителя, создают раздел, на который кладут ESXi. В результате получается своего рода дистрибутив ESXi на специальном носителе. Аналогичный подход применяют также, например, при создании СДЗ, которое может обеспечить доверенную загрузку нескольких серверов [11]. Раздел с ESXi по умолчанию установлен в режим RO. При запуске сервера сначала стартует специальное ПО носителя, которое затем передаёт управление ESXi, если загрузка не была прервана.

Обновления ESXi можно провести в двух режимах: автоматическом и ручном (подробнее об этом можно прочитать в документации ESXi [12]). При автоматическом обновлении ESXi будет запущен и установит предварительно помещённые на другой раздел носителя обновления своими штатными средствами. Недостаток этого метода состоит в том, что ESXi будет загружен с раздела, который можно изменять. При ручном методе данные для обновления можно записать на раздел с ESXi, не запуская сам гипервизор. Для этого необходимо посредством ПО на загрузочном разделе носителя загрузить не сам ESXi, а предварительно подготовленный раздел с обновле-

ниями. В любом случае при необходимости обновления перед стартом ESXi при помощи ПО носителя раздел временно переводят в режим RW (для перевода необходимо ввести пин-код). После установки обновлений сервер перезагружают, а раздел с ESXi вновь устанавливают в режим RO. Далее можно вновь загрузить ESXi уже с неизменяемого раздела и продолжить работу сервера в штатном режиме.

При наличии нужного числа USB-портов для подключения ещё и аппаратного идентификатора носитель со специальным ПО и ESXi можно дополнить СДЗ, выделив на носители разделы под ОС СДЗ и базу данных. При таком решении перед стартом ESXi будет сначала запускаться СДЗ для обеспечения доверенной загрузки гипервизора. Преимущество перед решением, использующим только СДЗ (например, Инаф), заключено в наличии неизменяемого раздела, с которого запускается ESXi. СДЗ может обеспечить только доверенную загрузку, а состояние сервера в процессе его работы СДЗ не контролирует. При данном решении загрузка с изменяемого раздела производится только для установки обновлений в автоматическом режиме. Схема такого носителя приведена на рис. 3.

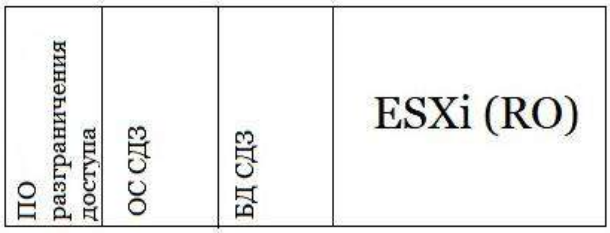


Рис. 3. Схема носителя с ПО разграничения доступа, СДЗ и ESXi

Разделы со специальным ПО и ESXi на носителе должны присутствовать обязательно, раздел с СДЗ — опционально. Если планируется проводить ручную установку обновлений, то также необходимо создать раздел, на который будут помещаться обновления.

Сценарий работы устройства таков:

- запуск специального ПО, расположенного на первом разделе носителя;
- в случае, если в течение определённого времени загрузка не была прервана, загрузка ESXi со своего раздела;
- прерывание загрузки после старта специального ПО может позволить:
  - перевести раздел с ESXi из режима RO в режим RW и обратно,
  - продолжить загрузку не с ESXi-раздела, а с раздела с обновлениями;
- при наличии СДЗ специальное ПО передаёт управление не загрузчику ESXi, а СДЗ, которое после успешного прохождения процедур идентификации-аутентификации и контроля целостности уже передаёт управление загрузчику ESXi.

Обсуждение

Данное решение применимо при условии, что сервер находится внутри контролируемой зоны, а загрузка с иных носителей или без установленного защищённого загрузочного носителя невозможна. Иначе у потенциального нарушителя будет возможность извлечь загрузочный носитель и вставить в сервер свой. Решение, не включающее СДЗ, требует одного свободного USB-слота, включающее — двух, но при этом не требует наличия PCI-слотов и возможности прошивать BIOS сервера. Расположение гипервизора на неизменяемом в основном режиме работы разделе гарантирует целостность гипервизора, а возможность перевода раздела с гипервизором в режим RW даёт возможность обновления. Безопасность обновления обеспечивает либо загрузка с раздела с обновлениями, либо проверка целостности раздела с гипервизором. При подобной схеме работы у злоумышленника нет возможности внедрить вредоносное ПО ни во время работы гипервизора, ни во время его обновления.

Заключение

Предложено решение, обеспечивающее защиту гипервизора от несанкционированного доступа на основе создания ДСС. Это решение позволит обеспечить целостность раздела с ESXi, возможность безопасного обновления гипервизора в ручном режиме и будет требовать наличия всего одного свободного USB-порта. Решение, включающее в себя СДЗ, по-

требует дополнительный USB-порт для подключения аппаратного идентификатора, но компенсирует этот недостаток возможностью провести доверенную загрузку ESXi с изменяемого раздела для автоматического обновления. При выполнении организационных и технических требований, возникающих из-за ограничений применимости, данное решение будет актуальным для компаний, использующих сервера с расположенными на них виртуальными машинами, безопасность подключения к которым необходимо обеспечить.

Литература

1. *Мозолина Н. В.* Защита виртуализации "в эпоху бурного развития" // Информационная безопасность. 2019. № 1. С. 29.
2. *Каннер А. М.* Разграничение доступа в Linux при использовании средства виртуализации kvm // Вопросы защиты информации. 2019. № 3. С. 3—7.
3. *Маляревский А.* Виртуализация как тренд 2020 [Электронный ресурс]. URL: https://www.crn.ru/news/detail.php?ID=141879
4. Сравнение гипервизоров: KVM, Hyper-V или VMware? [Электронный ресурс]. URL: https://www.xelent.ru/blog/sravnenie-gipervizorov-kvm-hyper-v-ili-vmware/
5. Что изменилось в структуре дисковых разделов (Partition Layout) на платформе WMware vSphere 7? [Электронный ресурс]. URL: https://www.vmgu.ru/news/vmware-vsphere-7-disk-partition-layout
6. *Конявский В. А.* Управление защитой информации на базе СЗИ НСД "Аккорд". — М.: Радио и связь, 1999. — 325 с.
7. *Каннер А. М.* Средство организации доверенного сеанса как альтернатива доверенной вычислительной среде // Информационные технологии управления в социально-экономических системах. 2010. Вып. 4. С. 140—143.
8. *Конявский В. А.* Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем — на старт, внимание, МАРШ!: мат. XV Междунар. науч.-практ. конф. "Комплексная защита информации". (Иркутск), 1—4 июня 2010 г.
9. *Чугринов А. В.* Доверенные сеансы связи и средства их обеспечения // Информационная безопасность. 2010. № 4. С. 54—55.
10. *Алтухов А. А.* Неатомарный взгляд на РКБ как на композицию перехвата управления и контроля целостности: материалы XX науч.-практ. конф. "Комплексная защита информации", Минск, 19—21 мая 2015. С. 53—55.
11. *Алтухов А. А.* Концепция персонального устройства контроля целостности вычислительной среды // Вопросы защиты информации. 2014. № 4. С. 64—68.
12. VMware ESXi Upgrade [Электронный ресурс]. URL: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.upgrade.doc/

Trusted communication session approaches and tools application for the safe operation of hypervisors in virtualization systems

A. D. Khmelkov
OKB SAPR, Moscow, Russia

Methods of protecting hypervisors from unauthorized changes to their images are considered. A new method of protection is proposed.

Keywords: hypervisors, ESXi, unauthorized access, trusted boot, trusted communication session.

Bibliography — 12 references. *Received December 11, 2020*

Электронная подпись в информационных системах

УДК 003.26

DOI: 10.52190/2073-2600_2021_1_16

Протокол слепой подписи, основанный на скрытой задаче дискретного логарифмирования в коммутативной алгебре

Д. Н. Молдовян, канд. техн. наук; *А. А. Костина; А. А. Курышева*
Санкт-Петербургский федеральный исследовательский центр РАН (СПб ФИЦ РАН),
Санкт-Петербург, Россия

Предложена новая схема слепой подписи, отличающаяся тем, что она основана на скрытой задаче дискретного логарифмирования, заданной в конечной коммутативной ассоциативной алгебре. Используемая алгебраическая основа представляет собой 4-мерную коммутативную ассоциативную алгебру, определенную над основным конечным полем GF (p), коммутативная группа которого обладает 4-мерной цикличностью. Открытый ключ представляет собой тройку векторов, принадлежащих различным циклическим подгруппам мультипликативной группы. Соответственно для обеспечения свойства анонимности предложенного протокола слепой подписи используются три различных ослепляющих множителя.

Ключевые слова: информационная безопасность, постквантовая криптография, цифровая подпись, слепая подпись, конечная ассоциативная алгебра, коммутативная алгебра, многомерная цикличность.

Схемы электронной цифровой подписи (ЭЦП) широко используют в информационных технологиях для решения различных задач обеспечения информационной безопасности [1, 2]. Ряд протоколов ЭЦП, обладающих различными свойствами, описан в литературных источниках [3, 4], в том числе протоколы мультиподписи [5, 6]. Особый интерес для применения в системах и в системах тайного электронного голосования представляет тип протоколов ЭЦП, называемый слепыми подписями [7, 8]. Специфическими требованиями к протоколам слепой ЭЦП являются отсутствие у подписывающего лица:

- доступа к документу в ходе процедуры формирования подписи;
- возможности найти корреляцию подписанного документа с актом подписания (требование анонимности или неотслеживаемости).

Для выполнения первого требования может быть использовано множество различных известных схем ЭЦП. Для этого достаточно принять соглашение о том, что подпись к документу формируется как подпись к хэш-функции, вычисляемой из документа. Первое требование является обязательным условием выполнимости второго требования. Для реализации протокола ЭЦП, удовлетворяющего второму требованию, применяют специфический метод, заключающийся в использовании ослепляющего множителя (или множителей) в ходе выполнения вычислений, предписываемых протоколом.

Участниками протокола слепой ЭЦП являются подписант (подписывающая сторона) и клиент, подготовивший к подписанию электронный документ. Протоколы такого типа ориентированы на использование в информационных технологиях, где подписант выполняет подписание множества документов, предоставляемых многими клиентами. Цель каждого конкретного клиента состоит в том,

Молдовян Дмитрий Николаевич, научный сотрудник.
E-mail: mdn.spectr@mail.ru
Костина Анна Александровна, научный сотрудник.
E-mail: anya@hotbox.ru
Курышева Алена Андреевна, аспирант.
E-mail: kurysheva.al@yandex.ru

Статья поступила в редакцию 18 февраля 2021 г.

чтобы получить подлинную подпись подписанта к подготовленному им документу таким образом, чтобы в будущем, когда подписанный документ будет представлен подписанту, последний не смог бы определить, кто из клиентов связан с этим документом.

Первый протокол слепой подписи [9] разработан на основе схемы подписи RSA [3], основанной на вычислительной сложности задачи факторизации (ЗФ). Впоследствии предложены протоколы слепой ЭЦП, основанные на вычислительной сложности задачи дискретного логарифмирования (ЗДЛ) [10]. В первом случае анонимность заявителя обеспечивается с помощью введения им в слепую подпись одного ослепляющего множителя, во втором — двух ослепляющих множителей. Протоколы разработаны таким образом, что подписант, используя свой личный секретный ключ, формирует слепую подпись и передает ее клиенту. После получения слепой подписи клиент удаляет ослепляющие множители, благодаря чему получает подлинную подпись.

Как и в случае современных стандартов ЭЦП и других широко используемых схем ЭЦП, основанных на вычислительной сложности ЗФ и ЗДЛ, указанные протоколы слепой подписи будут небезопасны в наступающей постквантовой эпохе [11, 12], когда квантовые атаки (атаки с использованием вычислений на квантовом компьютере) станут возможными на практике. Криптосхема называется постквантовой, если она эффективно работает на обычных компьютерах и противостоит квантовым атакам.

Постквантовые криптографические алгоритмы и протоколы должны основываться на вычислительно сложных задачах, отличных от ЗФ и ЗДЛ, поскольку для их решения существуют известные полиномиальные алгоритмы [13, 14] для квантового компьютера. Квантовый метод решения ЗФ и ЗДЛ использует: предельную эффективность выполнения дискретного преобразования Фурье периодической функции, принимающей значения в явно заданной конечной циклической группе; сведение каждой из упомянутых двух задач к задаче нахождения длины периода периодической функции [15, 16].

Откликом на данную проблему в области прикладной и теоретической криптографии стало объявление Национальным институтом стандартов и технологий США (NIST) в декабре 2016 г. программы принятия постквантовых криптографических стандартов распределения открытых ключей и схем цифровой подписи к 2024 г. [17]. В качестве основной части этой программы начат всемирный конкурс на разработку постквантовых криптосхем с открытым ключом [18]. Программа NIST не предусматривает разработку постквантовых прото-колов слепой подписи. Однако эта задача достаточно важна.

Данная работа посвящена разработке практической постквантовой схемы слепой подписи, основанной на вычислительной сложности так называемой скрытой задачи дискретного логарифмирования (СЗДЛ). Кратко описана концепция СЗДЛ как постквантового криптографического примитива и конечных ассоциативных алгебр (КАА) как алгебраической поддержки криптосхем с открытым ключом на основе СЗДЛ. Представлена исходная схема подписи на основе СЗДЛ, подходящая для преобразования в схему слепой подписи. В качестве алгебраического носителя разработанной схемы подписи использована новая 4-мерная коммутативная КАА с 4-мерной цикличностью. Предложен практичный постквантовый протокол слепой подписи, в котором используются три ослепляющих множителя и открытый ключ, представляющий собой тройку 4-мерных векторов.

Предварительные сведения

СЗДЛ рассматривают как один из привлекательных криптографических примитивов для разработки практических постквантовых криптосхем с открытым ключом. На основе СЗДЛ разработаны протоколы распределения открытых ключей [19, 20], алгоритмы коммутативного шифрования [21, 22] и схемы ЭЦП [23, 24]. Чтобы раскрыть понятие СЗДЛ, необходимо рассмотреть определение ЗДЛ.

Последняя обычно обозначается в заданной конечной циклической группе простого порядка q как нахождение неизвестного значе-

ния целого числа x в уравнении $Y' = G'^{x}$, где G' — генератор группы. СЗДЛ задается в конечной алгебраической структуре, содержащей очень большое количество различных циклических групп в виде различных подмножеств алгебраических элементов. Одна из таких групп выбирается случайным образом и является секретной (например, циклическая группа, образованная элементом G). Генерируется случайное неотрицательное целое число $x < q$ и рассчитывается значение $Y' = G$. Затем значения Y' и G отображаются в элементы $Y = \alpha(Y')$ и $Z = \beta(G)$, где $\alpha(Y')$ и $\beta(G)$ — маскирующие операции, обладающие свойством взаимной коммутативности с операцией возведения в степень. Параметры маскирующих операций являются секретными. СЗДЛ заключается в нахождении значения x, когда заданы элементы Y и Z. Предложены различные формы СЗДЛ для разработки различных открытых ключей. В некоторых частных формах СЗДЛ маскируется только одно из значений Y' и G [19, 25].

Конечные ассоциативные алгебры используют в качестве алгебраических носителей криптосхем на основе СЗДЛ. Произвольный вектор $\mathbf{A}$ некоторого конечного m-мерного векторного пространства, определенного над конечным полем, например над основным полем $GF(p)$, может быть записан как упорядоченное множество элементов поля $GF(p)$: $\mathbf{A} = (a_0, a_1, \ldots, a_{m-1})$, или как сумма его компонент: $\mathbf{A} = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, где $\mathbf{e}_i$ — базисные векторы; $a_i \in GF(p)$ — координаты вектора. Алгеброй называется векторное пространство, в котором помимо операций сложения векторов и умножения вектора на скаляр определена операция умножения двух векторов (векторное умножение), обладающая свойством дистрибутивности по отношению к операции сложения.

Операция умножения векторов $\mathbf{A} = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$ и $\mathbf{B} = \sum_{j=0}^{m-1} b_j \mathbf{e}_j$ обычно определяется с помощью правила умножения каждой составляющей первого вектора на каждую составляющую второго вектора по формуле

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

в которой каждое произведение вида $\mathbf{e}_i \circ \mathbf{e}_j$ должно быть заменено на однокомпонентный вектор $\lambda \mathbf{e}_k$, выбранный из так называемой таблицы умножения базисных векторов (ТУБВ), где $\lambda \in GF(p)$ представляет собой структурную постоянную. При $\lambda = 1$ в ТУБВ указывается только базисный вектор $\mathbf{e}_k$. Левый множитель в произведении $\mathbf{e}_i \circ \mathbf{e}_j$ обозначает строку, а правый — столбец. Их пересечение указывает на ячейку, содержащую значение $\lambda \mathbf{e}_k$.

С учетом формулы (1) можно доказать, что заданная операция умножения векторов является ассоциативной, если используемая ТУБВ такова, что для всех возможных троек $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$ выполняется равенство

$$\left(\mathbf{e}_i \circ \mathbf{e}_j \right) \circ \mathbf{e}_k = \mathbf{e}_i \circ \left(\mathbf{e}_j \circ \mathbf{e}_k \right). \qquad (2)$$

Если операция умножения векторов, заданная с помощью ТУБВ, обладает свойствами коммутативности (некоммутативности) и ассоциативности, то имеет место задание коммутативной (некоммутативной) КАА. Большинство различных известных форм СЗДЛ предложено для некоммутативных алгебр, используемых в качестве алгебраического носителя разрабатываемых криптосхем. В работе [22] приведен унифицированный метод задания некоммутативных КАА произвольных четных размерностей $m \geq 2$. В [26] представлен еще один унифицированный метод задания некоммутативных КАА другого типа произвольных четных размерностей $m > 4$. Для случая $m > 4$ последний метод определяет коммутативную КАА, обладающую многомерной цикличностью. Эта 4-мерная КАА использована в [27], чтобы впервые задать СЗДЛ в коммутативных алгебрах. Понятие многомерной цикличности предложено в [29]: коммутативная конечная группа, порожденная

минимальной системой образующих (базисом), содержащей $\mu \geq 2$ элементов одного порядка, называется группой, обладающей μ-мерной цикличностью.

В данной работе другая форма СЗДЛ задается в коммутативной КАА для создания постквантовой схемы подписи, которая подходит для разработки на ее основе постквантового протокола слепой подписи. Как и в случае схемы ЭЦП из [27], предложенная форма СЗДЛ использует многомерное циклическое строение мультипликативной группы коммутативной КАА, используемой в качестве алгебраического носителя криптосхемы. Однако предложенная форма реализует иной критерий постквантовой стойкости, чем в работе [27]. Это различие дает возможность разработать схему подписи, свободную от удвоения проверочного уравнения. Благодаря последнему появилась возможность разработать протокол слепой подписи на основе СЗДЛ, которая к тому же имеет меньший размер. В качестве алгебраического носителя заданной СЗДЛ и разработанных схем подписи использована новая 4-мерная коммутативная КАА.

Исходная схема подписи

Коммутативная 4-мерная КАА, используемая в качестве алгебраического носителя, задается над простым конечным полем $GF(p)$ с помощью ТУБВ, показанной в табл. 1.

Таблица 1

Задание 4-мерной коммутативной КАА, обладающей многомерной цикличностью ($\lambda = 4$)

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\lambda\,\mathbf{e}_3$	$\mathbf{e}_2$	$\lambda\,\mathbf{e}_1$	$\mathbf{e}_0$
$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_2$	$\lambda\,\mathbf{e}_1$	$\mathbf{e}_0$	$\lambda\,\mathbf{e}_3$	$\mathbf{e}_2$
$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$

Единицей этой ассоциативной алгебры является вектор $\mathbf{E}$ = (0, 0, 0, 1). Действительно, используя формулу (1) и табл. 1, можно легко продемонстрировать, что для всех 4-мерных векторов $\mathbf{V}$ справедливо каждое из уравнений $\mathbf{V} = \mathbf{V} \circ \mathbf{E}$ и $\mathbf{V} = \mathbf{E} \circ \mathbf{V}$. Векторы $\mathbf{V}$, для которых векторное уравнение $\mathbf{V} \circ \mathbf{X} = \mathbf{E}$ имеет единственное решение, называют обратимыми векторами. Для фиксированного вектора $\mathbf{V}$ решение обозначается как $\mathbf{V}^{-1}$ и называется обратным $\mathbf{V}$. Очевидно, что $\mathbf{V} \circ \mathbf{V}^{-1} = \mathbf{V}^{-1} \circ \mathbf{V} = \mathbf{E}$.

Множество всех обратимых векторов составляет конечную коммутативную группу, называемую мультипликативной группой алгебры. Как и в случае коммутативной КАА, приведенной в [27], указанная группа имеет 4-мерную (2-мерную) цикличность, если структурная константа λ равна квадратичному вычету (невычету) в поле $GF(p)$. В случае образования группы с 2-мерной цикличностью ее базис включает два вектора, каждый из которых имеет порядок, равный $p^2 - 1$, а ее порядок равен $(p^2 - 1)^2$. В табл. 2 и 3 приведены некоторые примеры векторов $\mathbf{V}$, имеющих максимально возможный порядок для указанных двух случаев значения структурной константы λ, когда p = 14377379 (q = 7188689).

Таблица 2

Векторы V, имеющие максимальный порядок, равный $p - 1$ (λ — квадратичный вычет)

λ	$\mathbf{V}$
4	(10783034; 7188689; 13594345; 7188689)
9	(9415710; 3572423; 13398841; 13983581)
25	(11981149; 7188690; 7981149; 7188689)
3	(6125368; 2977015; 8115131; 2640973)
5	(11036650; 1231043; 3719781; 1538072)

Таблица 3

Векторы V, имеющие максимальный порядок $p^2 - 1$ (λ — квадратичный невычет)

λ	$\mathbf{V}$
2	(6849615; 14075541; 12012209; 2434744)
7	(3056942; 11995808; 6447316; 5237791)
8	(1610296; 14317805; 11296173; 5273238)
11	(10918357; 12126862; 11033630; 3625780)
17	(1858503; 1987085; 7520796; 3040436)

При разработке схемы ЭЦП на основе СЗДЛ используем случай 4-мерной цикличности, когда базис мультипликативной группы Г включает четыре вектора, каждый из которых имеет порядок $p - 1$. При этом порядок группы Г равен $(p - 1)^4$. Предполагается также, что $\lambda = 4$ и характеристика p поля $GF(p)$ равна простому числу, имеющему структуру $p = 2q + 1$, где q — специально подобранное 512-битное простое число. Генерация требуемых простых чисел p осуществляется путем генерации множества различных 512-битных простых чисел q и проверки значений $p = 2q + 1$ на простоту.

В табл. 4 приведены примеры простых значений q различного размера, для которых значение $2q + 1$ является простым.

Для разработки схемы ЭЦП на основе СЗДЛ используем примарную группу порядка q^4, содержащуюся в мультипликативной группе алгебры (примарной называется группа, порядок которой равен степени простого числа). Для генерации базиса этой группы $<\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_3, \mathbf{G}_4>$ может быть использован вероятностный метод, описанный в [27]. Этот метод предполагает генерацию случайных четырех векторов порядка q, которые с вероятностью около $1 - q^{-1}$ образуют базис упомянутой примарной группы. Предположим, что получены четыре вектора, $\mathbf{G}_1$, $\mathbf{G}_2$, $\mathbf{G}_3$ и $\mathbf{G}_4$, составляющие базис примарной группы порядка q^4.

Процедура создания открытого ключа в разработанной схеме подписи включает следующие этапы:

- сгенерировать случайным образом два неотрицательных целых числа $x < q$ и $w < q$;
- вычислить вектор $\mathbf{Y} = \mathbf{G}_1^{x} \circ \mathbf{G}_2^{w}$;
- вычислить вектор $\mathbf{Z} = \mathbf{G}_1 \circ \mathbf{G}_3^{1/x}$;
- вычислить вектор $\mathbf{U} = \mathbf{G}_2 \circ \mathbf{G}_3^{-1/w}$.

Полученный открытый ключ представляет собой тройку 4-мерных векторов (**Y**, **Z**, **U**), содержащихся в трех различных циклических подгруппах первичной группы.

Алгоритм генерации ЭЦП:

- сгенерировать случайным образом неотрицательное целое число $k < q$;
- вычислить целое число $t = kwx^{-1} \bmod q$;
- вычислить вектор $\mathbf{R} = \mathbf{G}_1^{k} \circ \mathbf{G}_2^{t}$;
- вычислить первый элемент подписи $e = f_h(M, \mathbf{R})$, где f_h — предварительно согласованная 512-битная хэш-функция, удовлетворяющая требованию коллизионной стойкости; M — подписываемый документ;
- вычислить второй элемент подписи: $s = k - ex \bmod q$;
- вычислить третий элемент подписи: $d = t - ew \bmod q$.

Этот алгоритм вырабатывает 1536-битную подпись в виде тройки 512-битных целых чисел (e, s, d).

Процедура проверки подлинности подписи (e, s, d) к документу M выполняется с использованием открытого ключа (**Y**, **Z**, **U**) следующим образом.

Таблица 4

Специально подобранные простые значения q

q (длина в битах)	p
1156112201(32)	2312224403
6785973453813842891 (64)	13571946907627685783
15777278116070701 3851236586330907166231 (128)	31554556232141402770 2473172661814332463
294376761264963048730708277251 2639408627270785989333 59355149534238513219915l9(256)	588753522529926097461416554 5 0252788172545415719786671 8710299068477026439830 39
35687538543572407882858303216507 61155407334331566376142966145846 64045696352628128923744450422769 90309175242333397008877768843061 17702415790074075810133363 (512)	71375077087144815765716606433015 22310814668663132752285932 29 16932809139270525625784748890 0 84553980618350484666794017755537 68612235404831580148151620266727

Алгоритм проверки подписи:

- вычислить вектор $\mathbf{R^*} = \mathbf{Y}^{e} \circ \mathbf{Z}^{s} \circ \mathbf{U}^{d}$;
- вычислить хэш-значение $e^* = f_h(M, \mathbf{R^*})$;

если $e^* = e$, то подпись считается подлинной. В противном случае подпись отклоняется как поддельная.

Рассмотрим подпись (e, s, d) к документу M, которая была правильно вычислена в полном соответствии с алгоритмом генерации подписи. Для доказательства корректности разработанной схемы ЭЦП покажем, что указанная подпись проходит процедуру проверки как подлинная:

$$\mathbf{R}^* = \mathbf{Y}^e \circ \mathbf{Z}^s \circ \mathbf{U}^d =$$

$$= \mathbf{G}_1^{xe} \circ \mathbf{G}_2^{we} \circ \mathbf{G}_1^{k-xe} \circ \mathbf{G}_3^{x^{-1}(k-ex)} \circ$$

$$\circ \mathbf{G}_2^{t-we} \circ \mathbf{G}_3^{-w^{-1}(t-ex)} = \mathbf{G}_1^{k} \circ \mathbf{G}_2^{t} \circ \mathbf{G}_3^{x^{-1}k-e-w^{-1}t+e} =$$

$$= \mathbf{G}_1^{k} \circ \mathbf{G}_2^{t} \circ \mathbf{G}_3^{x^{-1}k-w^{-1}\left(x^{-1}kw\right)} = \mathbf{G}_1^{k} \circ \mathbf{G}_2^{t} =$$

$$= \mathbf{R} \Rightarrow f_h\left(M, \mathbf{R}^*\right) = f_h\left(M, \mathbf{R}\right) \Rightarrow e^* = e.$$

Заметим, что владелец открытого ключа (**Y**, **Z**, **U**) имеет возможность использовать альтернативный метод вычисления подписи, который аналогичен описанному алгоритму генерации ЭЦП за исключением третьего шага. Последний в альтернативном алгоритме генерации подписи выглядит следующим образом: вычислить вектор $\mathbf{R} = \mathbf{Z}^k \circ \mathbf{U}^t$.

Поскольку $\mathbf{Z}^k \circ \mathbf{U}^t = \mathbf{G}_1^k \circ \mathbf{G}_2^t$, альтернативный алгоритм вычисления сигнатуры работает правильно и позволяет использовать только два 512-битных целых числа, x и w, в качестве 1024-битного закрытого ключа вместо использования четырех секретных значений, x, w, $\mathbf{G}_1$ и $\mathbf{G}_2$, в качестве 5120-битного закрытого ключа.

Протокол слепой подписи

Как и в известных схемах подписи на основе ЗДЛ, в подписи, разработанной на основе СЗДЛ, основной вклад в стойкость вносят операции возведения в степень, выполняемые во время процедур генерации открытого ключа, вычисления подписи и проверки подписи. Однако принципиальным отличием последней являются следующие два момента: при вычислении открытого ключа операции возведения в степень выполняются в двух различных конечных циклических группах; эти группы скрыты за счет маскирующих умножений на векторы $\mathbf{G}_3^{1/x}$ и $\mathbf{G}_3^{-1/w}$ из третьей циклической группы. В связи с заметными отличиями разработанной схемы ЭЦП элементы открытого ключа (Y, Z, U) относятся к трем различным циклическим группам.

Предложенное уравнение проверки подписи $\mathbf{R}^* = \mathbf{Y}^e \circ \mathbf{Z}^s \circ \mathbf{U}^d$ включает множители трех типов. Поэтому в протоколе слепой подписи, основанном на схеме подписи, разработанной на основе СЗДЛ, следует использовать ослепляющие множители трех различных типов: $\mathbf{Y}^{\varepsilon}$, $\mathbf{Z}^{\sigma}$ и $\mathbf{U}^{\tau}$. Таким образом, как и в случае известных протоколов слепой ЭЦП на основе ЗДЛ [6, 10, 30], клиент, участвующий в процессе создания слепой подписи, должен выполнить генерацию трех равномерно случайных целых чисел, $\varepsilon < q$, $\sigma < q$ и $\tau < q$, с последующим вычислением указанных трех ослепляющих множителей.

Предложенный протокол слепой цифровой подписи на основе СЗДЛ включает в себя следующие этапы:

- подписант генерирует случайное неотрицательное целое число $k < q$ и вычисляет целое число $t = kwx^{-1} \bmod q$. Затем он вычисляет вектор $\bar{\mathbf{R}} = \mathbf{Z}^{x} \circ \mathbf{U}^{t}$. Далее подписант посылает значение $\bar{\mathbf{R}}$ клиенту, который хочет получить подлинную подпись подписанта к документу M (содержимое документа подписанту неизвестно);
- заявитель создает три равномерно случайных натуральных числа $\varepsilon < q$, $\sigma < q$ и $\tau < q$, вычисляет вектор $\mathbf{R} = \bar{\mathbf{R}} \circ \mathbf{Y}^{\varepsilon} \circ \mathbf{Z}^{\sigma} \circ \mathbf{U}^{\tau}$ и первый элемент e подлинной подписи подписанта $e = f_h(M, \mathbf{R})$;
- заявитель вычисляет первый элемент слепой подписи $\bar{e} = e - \varepsilon \bmod q$ и отправляет его подписанту;
- используя свой закрытый ключ (x, w), подписант вычисляет второй ($\bar{s}$) и третий ($\bar{d}$) элементы слепой подписи: $\bar{s} = k - \bar{e}x \bmod q$ и

$\bar{d} = t - \bar{e}w \bmod q$. Затем он отправляет значения $\bar{s}$ и $\bar{d}$ клиенту;

- используя значения $\bar{s}$ и $\bar{d}$, клиент вычисляет второй (s) и третий (d) элементы подлинной подписи подписанта к документу M: $s = \bar{s} + \sigma \bmod q$ и $d = \bar{d} + \tau \bmod q$.

Процедура проверки подписи (e, s, d) к документу M выполняется с помощью использования открытого ключа (**Y**, **Z**, **U**) и алгоритма проверки подписи исходной схемы подписи на основе СЗДЛ, описанной ранее.

Корректность работы описанного протокола слепой подписи может быть доказана путем подстановки подписи на вход процедуры проверки подлинности ЭЦП и демонстрации того, что она проходит верификацию как подлинная.

Доказательство корректности протокола слепой цифровой подписи на основе вычислительной сложности СЗДЛ выполняется следующим образом:

$$\mathbf{R}^* = \mathbf{Y}^e \circ \mathbf{Z}^s \circ \mathbf{U}^d = \mathbf{Y}^{\bar{e}+\varepsilon} \circ \mathbf{Z}^{\bar{s}+\sigma} \circ \mathbf{U}^{\bar{d}+\tau} =$$

$$= \mathbf{Y}^{\bar{e}} \circ \mathbf{Z}^{\bar{s}} \circ \mathbf{U}^{\bar{d}} \circ \mathbf{Y}^{\varepsilon} \circ \mathbf{Z}^{\sigma} \circ \mathbf{U}^{\tau} =$$

$$= \bar{\mathbf{R}} \circ \mathbf{Y}^{\varepsilon} \circ \mathbf{Z}^{\sigma} \circ \mathbf{U}^{\tau} = \mathbf{R} \Rightarrow$$

$$\Rightarrow f_h\left(M, \mathbf{R}^*\right) = f_h\left(M, \mathbf{R}\right) \Rightarrow e^* = e.$$

Чтобы показать, что описанный протокол обеспечивает анонимность, рассмотрим некоторую слепую подпись ($\bar{e}$, $\bar{s}$, $\bar{d}$) и произвольную подлинную подпись (e, s, d). Для этих двух подписей можно записать

$$\left.\begin{cases} \mathbf{R} = \mathbf{Y}^e \circ \mathbf{Z}^s \circ \mathbf{U}^d \\ \bar{\mathbf{R}} = \mathbf{Y}^{\bar{e}} \circ \mathbf{Z}^{\bar{s}} \circ \mathbf{U}^{\bar{d}} \end{cases}\right\} \Rightarrow$$

$$\Rightarrow \mathbf{R} = \bar{\mathbf{R}} \circ \mathbf{Y}^{e-\bar{e}} \circ \mathbf{Z}^{s-\bar{s}} \circ \mathbf{U}^{d-\bar{d}}.$$

Таким образом, подписи ($\bar{e}$, $\bar{s}$, $\bar{d}$) и (e, s, d) связаны через некоторые случайные величины $\varepsilon = e - \bar{e}$; $\sigma = s - \bar{s}$ и $\tau = d - \bar{d}$. Поэтому имея заданную подлинную подпись, подписант не может идентифицировать слепую подпись, связанную с данной подлинной подписью.

Обсуждение полученных результатов

Впервые реализация схем подписи на основе ЗДЛ на коммутативных КАА была предложена в работе [27]. Основными общими особенностями схем ЭЦП, представленных в данной статье и в [27], являются следующие:

- коммутативная мультипликативная группа КАА, используемая в качестве алгебраической основы схемы подписи, обладает 4-мерной цикличностью;
- для обеспечения устойчивости к квантовым атакам используется вычислительная сложность СЗДЛ.

Указанные две схемы ЭЦП имеют ряд существенных отличий, которые обусловлены использованием различных критериев для обеспечения постквантовой стойкости. Схема подписи из [27] соответствует общему критерию постквантовой стойкости, введенному в [28], который можно сформулировать следующим образом: *схему подписи следует построить таким образом, чтобы задание периодических функций на основе открытых параметров схемы, содержащих период с длиной, зависящей от значения дискретного логарифма, представляло собой вычислительно сложную задачу.*

Чтобы удовлетворить указанному конструктивному критерию, ориентированному на обеспечение стойкости как к известному, так и к возможному в будущем квантовому алгоритму для нахождения длины периода периодических функций, в схеме подписи [27] использован метод удвоения уравнения проверки подлинности, подобный описанному в [28]. При этом один из элементов подписи представляет собой элемент алгебры. Из-за этих двух особенностей размеры открытого ключа и подписи в [27] довольно велики. Кроме того, неясно, как разработать протокол слепой подписи на основе схемы ЭЦП из [27].

В предложенной схеме подписи использован конкретный конструктивный критерий постквантовой стойкости, ориентированный на обеспечение безопасности от известных квантовых атак [13, 16], который был исполь-

зован в [22, 23] для разработки схем подписи на основе СЗДЛ на некоммутативных КАА. Можно предложить следующую формулировку используемого частного критерия: *периодическая функция f, заданная на основе открытых параметров схемы подписи и содержащая период с длиной, зависящей от значения дискретного логарифма, должна принимать значения в различных конечных циклических группах, содержащихся в алгебраической основе схемы подписи, и ни одна циклическая группа не может быть указана в качестве предпочтительной циклической группы для значений функции f.*

Можно задать периодическую функцию от трех целочисленных переменных, i, j и k, с периодом длины (hx^{-1}, h, hxw^{-1}), зависящей от значений x и w: $F(i, j, k) = \mathbf{Y}^{i} \circ \mathbf{Z}^{j} \circ \mathbf{U}^{k}$. Однако значения функции $F(i, j, k)$ лежат во многих различных циклических группах, содержащихся в примарной подгруппе порядка q^3, которая порождается базисом $\langle \mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_3 \rangle$. В то же время невозможно выделить какую-либо фиксированную циклическую группу, которая со значительной вероятностью включает в себя значения функции $F(i, j, k)$. Это обстоятельство не позволяет применить квантовый алгоритм Шора [13] для нахождения длины периода функции $F(i, j, k)$, а затем найти значения x и w.

Схемы подписи, описанные авторами ранее, характеризуются следующими особенностями:

- схема подписи задается в скрытой коммутативной группе с 2-мерной цикличностью, поэтому дискретный логарифм представляет собой пару целых чисел x и w (скрытая группа задается секретными векторами $\mathbf{G}_1$ и $\mathbf{G}_2$);
- элементы открытого ключа $\mathbf{Z}$ и $\mathbf{U}$ представляют собой замаскированные формы векторов $\mathbf{G}_1$ и $\mathbf{G}_2$, составляющих базис скрытой группы (маскирование реализуется как умножение на векторы $\mathbf{G}_3^{1/x}$ и $\mathbf{G}_3^{-1/w}$, содержащиеся в циклической группе, генерирующей вектор $\mathbf{G}_3$, который вместе с векторами $\mathbf{G}_1$ и $\mathbf{G}_2$ составляет базис примарной группы порядка q^3, обладающую 3-мерной цикличностью);
- степени маскирующих множителей $\mathbf{G}_3^{1/x}$ и $\mathbf{G}_3^{-1/w}$ выбираются таким образом, чтобы их вклад в левую часть проверочного уравнения сводился к умножению на единичный элемент алгебры (этот момент учитывается и при генерации рандомизирующих целочисленных значений k и t в процедуре генерации ЭЦП).

Разработанная схема подписи на основе СЗДЛ и протокол слепой подписи являются кандидатами на практичную постквантовую криптосистему с открытым ключом из-за достаточно малого размера открытого ключа и подписи (табл. 5).

Таблица 5

Сравнение подписи на основе СЗДЛ (для случая 512-битного значения *p*) с некоторыми известными схемами

Схема подписи	Размер подписи, байт	Размер открытого ключа, байт	Вычислительная сложность генерации подписи, умножения в $GF(p)$	Вычислительная сложность проверки подлинности (верификации) подписи, умножения в $GF(p)$
[27]	384	1024	4,608	3,072
[28]	384	1024	2,303	3,072
Предлагается в данной работе	192	768	1,536	2,304
Предлагаемый протокол слепой ЭЦП	192	768	3,840	2,304

Разработанная схема и протокол ЭЦП используют новую 4-мерную коммутативную КАА. Однако они могут быть реализованы с использованием 4-мерной коммутативной КАА, описанной в [27].

Заключение

Предложена новая схема подписи, основанная на вычислительной сложности СЗДЛ, заданной в коммутативной КАА, и использованная для разработки практичного постквантового протокола слепой подписи. Преимуществами предложенной схемы и протокола являются сравнительно небольшие размеры открытого ключа и подписи.

Работа выполнена при финансовой поддержке РФФИ (проект № 21-57-54001-Вьет_а).

Литература

1. *Chiou S. Y.* Novel Digital Signature Schemes based on Factoring and Discrete Logarithms // International J. Security and Its Applications. 2016. V. 10. № 3. P. 295—310.

2. Public-Key Cryptography — PKC 2019: 22nd IACR International Conference on Practice and Theory ofPublic-Key Cryptography, Beijing, China, April 14–17, 2019, Proceedings. Lecture Notes in Computer Science series. — Springer, 2019. V. 11443.

3. *Rivest R. L., Shamir A., Adleman L. M.* A Method for Obtaining Digital Signatures and Public Key Cryptosystems // Communications of the ACM. 1978. V. 21. № 2. P. 120—126.

4. *ElGamal T.* A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory. 1985. V. IT-31. № 4. P. 469—472.

5. *Boldyreva A.* Efficient Threshold Signature, Multisignature and Blind Signature Shemes Based on the Gap-Diffi-Hellman-Group Signature Sheme. — Springer-Verlag Lecture Notes in Computer Science. 2003. V. 2139. P. 31—46.

6. *Moldovyan D. N., Moldovyan N. A.* Blind Collective Signature Protocol Based on Discrete Logarithm Problem // Int. J. Network Security. 2011. V. 13. № 11. P. 22—30.

7. *Chaum D.* Security without identification: Transaction systems to make big brother obsolete // Communications of the AMS. 1985. V. 28. № 10. P. 1030—1044.

8. *Chaum D.* Blind Signature Systems. U.S. Patent № 4,759,063. 19 July 1988.

9. *Chaum D.* Blind Signatures for Untraceable Payments. Advances in Cryptology: Proc. of CRYPTO'82. PlenumPress, 1983. P. 199—203.

10. *Camenisch J. L., Piveteau J.-M., Stadler M. A.* Blind Signatures Based on the Discrete Logarithm Problem: Advances in Crypology — EUROCRYPT '94 volume 950 of LNCS, pages 428—432. — Springer Verlang, 1995.

11. *Yan S. Y.* Quantum Attacks on Public-Key Cryptosystems. — Springer US, 2014. — 207 p.

12. Post-Quantum Cryptography: 10-th International Conference, PQCrypto 2019, Chongqing, China, May 8—10, 2019, Proceedings. Lecture Notes in Computer Science series. — Springer, 2018. V. 11505.

13. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM J. Computing. 1997. V. 26. P. 1484—1509.

14. *Smolin J. A., Smith G., Vargo A.* Oversimplifying quantum factoring // Nature. 2013. V. 499. № 7457. P. 163—165.

15. *Jozsa R.* Quantum algorithms and the Fourier transform // Proc. Roy. Soc. London. Ser A. 1988. V. 454. P. 323—337.

16. *Ekert A., Jozsa R.* Quantum computation and Shor's factoring algorithm // Reviews of Modern Physics. 1996. V. 68. P. 733—752.

17. Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms [Электронный ресурс]. Режим доступа: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf

18. Post-Quantum Cryptography. Round 3 Submissions [Электронный ресурс]. Режим доступа: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (accessed January 10, 2020).

19. *Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.* Cryptographic Algorithms on Groups and Algebras // J. Mathematical Sciences. 2017. V. 223. № 5. P. 629—641.

20. *Moldovyan D. N.* Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem // Computer Science J. Moldova. 2019. V. 27. № 1(79). P. 56—72.

21. *Moldovyan D. N., Moldovyan N. A., Moldovyan A. A.* Commutative Encryption Method Based on Hidden Logarithm Problem // Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software. 2020. V. 13. № 2. P. 54—68. DOI: 10.14529/mmp200205.

22. *Moldovyan N. A., Moldovyan A. A.* Finite Noncommutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem // Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software. 2019. V. 12. № 1. P. 66--81. DOI: 10.14529/mmp190106.

23. *Moldovyan N. A., Abrosimov I. K.* Post-quantum electronic digital signature scheme based on the enhanced form of the hidden discrete logarithm problem // Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes. 2019. V. 15. № 2. P. 212—220. https://doi.org/10.21638/11702/spbu10.2019.205 (In Russian).

24. *Moldovyan N. A., Moldovyan A. A.* Candidate for practical post-quantum signature scheme // Vestnik of Saint

Petersburg University. Applied Mathematics. Computer Science. Control Processes. 2020. V. 16. № 4. P. 455—461. https://doi.org/10.21638/11701/spbu10.2020.410

25. *Moldovyan D. N.* Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes // Quasigroups and Related Systems. 2010. V. 18. P. 165—176.

26. *Moldovyan N. A.* Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // Quasigroups and Related Systems. 2020. V. 26. № 2. P. 263—270.

27. *Minh Nguyen Hieu, Moldovyan A. A., Moldovyan N. A., Canh Hoang Ngoc.* A New Method for Designing Post-Quantum Signature Schemes // J. Communications. 2020. V. 15. № 10. P. 747—754. Doi: 10.12720/jcm.15.10.747-754

28. *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.

29. *Moldovyan N. A., Moldovyanu P. A.* New primitives for digital signature algorithms // Quasigroups and Related Systems. 2009. V. 17. № 2. P. 271—282.

30. *Pointcheval D., Stern J.* Security Arguments for Digital Signatures and Blind Signatures // J. Cryptology. 2000. V. 13. № 3. P. 361—396.

Blind digital signature protocol on the base of hidden logarithm problem in a finite commutative algebra

D. N. Moldovyan, A. A. Kostina, A. A. Kurysheva
St. Petersburg Federal Research Centerof of the RAS (SPC RAS), St. Petersburg, Russia

A novel blind digital signature protocol is introduced, which is based on a hidden logarithm problem set in a finite 4-dimensional commutative algebra with associative multiplication operation. The used algebra is defined over the ground finite field GF (p). Multiplicative group of the algebra possesses 4-dimensional cyclicity. The public key is generated in the form of a triple of vectors that are generators of three different cyclic subgroups. Three blinding factors are used in the developed protocol to insure the anonymity property of the protocol.

Keywords: information security, post-quantum cryptography, digital signature, blind signature, finite associative algebra, commutative algebra, multi-dimensional cyclicity.

Bibliography — 30 references. *Received February 18, 2021*

УДК 003.26

DOI: 10.52190/2073-2600_2021_1_26

Задание шестимерных алгебр как носителей криптосхем, основанных на скрытой задаче дискретного логарифмирования

Д. Н. Молдовян, канд. техн. наук
Санкт-Петербургский федеральный исследовательский центр РАН (СПб ФИЦ РАН),
Санкт-Петербург, Россия

Рассмотрено строение ряда четырехмерных конечных некоммутативных ассоциативных алгебр (КНАА). Показаны некоторые проблемы с использованием необратимых элементов таких алгебр в качестве параметров схем цифровой подписи, основанных на скрытой задаче дискретного логарифмирования. Для устранения этих проблем предложено использование шестимерных и восьмимерных алгебр. Разработан унифицированный способ задания алгебр последнего типа.

Ключевые слова: информационная безопасность, постквантовая криптография, цифровая подпись, конечная ассоциативная алгебра, коммутативная алгебра, мультипликативные группы.

Скрытая задача дискретного логарифмирования (СЗДЛ) предложена в качестве базового примитива для построения постквантовых схем электронной цифровой подписи (ЭЦП) [1]. В работах [2—4] представлена реализация схем ЭЦП указанного типа при использовании в качестве алгебраического носителя четырехмерных конечных некоммутативных ассоциативных алгебр (КНАА), заданных над простым конечным полем $GF(p)$. При этом для устранения возможности сведения СЗДЛ к задаче дискретного логарифмирования в поле $GF(p)$ в качестве скрытой циклической группы используют необратимые элементы КНАА, которые содержат глобальную двухстороннюю единицу. Однако доля необратимых векторов в четырехмерных алгебрах составляет примерно p^{-1} от числа всех элементов алгебры, причем умножение на необратимый элемент обладает "сжимающим" свойством. Эти моменты делают актуальным рассмотрение строения четырехмерных КНАА для установления видов коммутативных мультипликативных групп, содержащихся в алгебрах, и определения числа групп каждого типа.

В настоящей работе рассмотрено строение ряда четырехмерных алгебр и показано, что при использовании скрытой циклической группы, генерируемой необратимым вектором, решение СЗДЛ может быть выполнено с использованием полиномиального квантового алгоритма [5]. В связи с этим предложено использовать шестимерные и восьмимерные КНАА с глобальной двухсторонней единицей. Разработан унифицированный способ задания класса таких алгебр.

Четырехмерные КНАА

В данной статье будем придерживаться описания КНАА и толкования понятия СЗДЛ, представленных в работах [3, 4]. Рассмотрим четырехмерные алгебры, заданные над полем $GF(p)$ с использованием таблиц умножения базисных векторов (ТУБВ), показанных как табл. 1—4. Благодаря использованию прореженных ТУБВ, умножение в этих алгебрах обладает сравнительно низкой вычислительной сложностью, что представляет интерес в плане повышения производительности алго-

Молдовян Дмитрий Николаевич, научный сотрудник.
E-mail: mdn.spectr@mail.ru

Статья поступила в редакцию 22 февраля 2021 г.

ритмов ЭЦП. Указанная особенность приведенных ТУБВ упрощает задачу детального изучения строения алгебр, что связано с более простой структурой систем уравнений, которые требуется проанализировать для описания коммутативных подалгебр.

Таблица 1

Задание первой четырехмерной КНАА ($\lambda \neq 0$) с глобальной двухсторонней единицей вида (0, 1, 1, 0)

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	0	0	$\mathbf{e}_0$	$\lambda\,\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_1$	0	0
$\mathbf{e}_2$	0	0	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\lambda\,\mathbf{e}_2$	$\mathbf{e}_3$	0	0

Таблица 2

Задание второй четырехмерной КНАА ($\lambda \neq 0$) с глобальной двухсторонней единицей вида (0, 0, 1, 1)

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	0	$\lambda\,\mathbf{e}_3$	$\mathbf{e}_0$	0
$\mathbf{e}_1$	$\lambda\,\mathbf{e}_2$	0	0	$\mathbf{e}_1$
$\mathbf{e}_2$	0	$\mathbf{e}_1$	$\mathbf{e}_2$	0
$\mathbf{e}_3$	$\mathbf{e}_0$	0	0	$\mathbf{e}_3$

Таблица 3

Задание четырехмерной КНАА ($\lambda \neq 0$) с глобальной двухсторонней единицей вида (1, 0, 0, 1)

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	0	0
$\mathbf{e}_1$	0	0	$\lambda\,\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\lambda\,\mathbf{e}_3$	0	0
$\mathbf{e}_3$	0	0	$\mathbf{e}_2$	$\mathbf{e}_3$

Таблица 4

Задание четырехмерной КНАА ($\lambda \neq 0$) с глобальной двухсторонней единицей вида (1, 1, 0, 0)

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	0	0	$\mathbf{e}_3$
$\mathbf{e}_1$	0	$\mathbf{e}_1$	$\mathbf{e}_2$	0
$\mathbf{e}_2$	$\mathbf{e}_2$	0	0	$\lambda\,\mathbf{e}_1$
$\mathbf{e}_3$	0	$\mathbf{e}_3$	$\lambda\,\mathbf{e}_0$	0

Для определения строения каждой из рассматриваемых алгебр применен метод выделения подмножеств взаимно коммутативных алгебраических элементов, включающий следующей этапы.

1. Составление системы линейных уравнений, описывающих все векторы, взаимно перестановочные с некоторым заданным вектором $\mathbf{A}=(a_0, a_1, a_2, a_3)$, т. е. соответствующие векторному уравнению вида

$$\mathbf{AX}-\mathbf{XA}=(0, 0, 0, 0);$$

где $\mathbf{X}=(x_0, x_1, x_2, x_3)$ — неизвестный вектор.

2. Выводится формула, описывающая множество взаимно перестановочных векторов, которое образует коммутативную подалгебру порядка p^2.

3. Подсчитывается число необратимых алгебраических элементов и выводится формула для порядка мультипликативной группы коммутативной подалгебры.

4. Показывается, что в зависимости от вида вектора $\mathbf{A}$, указанная мультипликативная группа относится к одному из трех возможных типов, различающихся значением порядка и строением. Тип коммутативной подалгебры определяется типом ее мультипликативной группы.

Для каждой из рассматриваемых четырехмерных КНАА характерны следующие три типа коммутативных подалгебр порядка p^2.

1. Подалгебры, мультипликативная группа (Γ_1) которых имеет циклическое строение и порядок, равный $\Omega_1 = p^2 - 1$. Подалгебра данного типа является полем $GF(p^2)$.

2. Подалгебры, мультипликативная группа (Γ_2) которых имеет двухмерное циклическое строение (ее базис включает два вектора, имеющих одно и то же значение порядка, равное $p-1$) и порядок, равный $\Omega_2 = (p-1)^2$. Подалгебра данного типа содержит $2p-1$ необратимых векторов, включая нулевой вектор.

3. Подалгебры, мультипликативная группа (Γ_3) которых имеет циклическое строение и

порядок, равный $\Omega_3 = p(p-1)$. Подалгебра данного типа содержит p необратимых векторов, включая нулевой вектор.

Для числа подалгебр первого η_1, второго η_2 и третьего η_3 типов получены следующие формулы:

$$\eta_1 = 2^{-1} p(p-1); \quad (1)$$

$$\eta_2 = 2^{-1} p(p+1); \quad (2)$$

$$\eta_3 = p+1. \quad (3)$$

Таким образом, четыре четырехмерные КНАА, заданные по табл. 1—4, имеют одинаковое строение. Можно предположить, что и другие четырехмерные КНАА обладают аналогичным строением, однако для каждой алгебры вопрос изучения строения требует самостоятельного рассмотрения. На основе результатов рассмотрения строения алгебр могут быть легко составлены процедуры генерации обратимых и необратимых векторов, принадлежащих подалгебрам указанных трех типов. В этих процедурах используются формулы, вид которых определяется выбором конкретной КНАА. Детальное рассмотрение этих процедур представляет отдельный интерес. В данной статье делается акцент на свойствах, которые характерны всем рассматриваемым четырехмерным алгебрам.

С точки зрения построения схем ЭЦП, основанных на вычислительной трудности СЗДЛ и использующих скрытую группу генерируемую некоторым необратимым вектором, представляет интерес рассмотрение множеств необратимых векторов, содержащихся в коммутативных подалгебрах второго и третьего типов. Пусть необратимый вектор $\mathbf{N}$ из подалгебры третьего типа генерирует циклическую группу, единицей которой является некоторый другой необратимый вектор $\mathbf{E}_\mathbf{N}$, для вычисления координат которого можно вывести математическую формулу (как это выполнено, например, в статьях [3, 6]).

Пусть всевозможные степени необратимого вектора $\mathbf{N}$ генерируют некоторую циклическую группу, включающую множество элементов $\{\mathbf{N}, \mathbf{N}^2, \ldots, \mathbf{N}^i, \ldots \mathbf{N}^\omega\}$, где $\mathbf{N}^\omega = \mathbf{E}_\mathbf{N}$ и $\omega \le p-1$ (нулевой вектор не содержится в этом множестве). Легко видеть, что формула $\mathbf{S}^k\mathbf{N} = \alpha^k\mathbf{N}$, где $\mathbf{S} = \alpha\mathbf{E}$ — вектор-скаляр; α — примитивный элемент в поле $GF(p)$, при $k = 0, 1, \ldots, p-1$ дает p различных необратимых векторов, перестановочных с $\mathbf{N}$, т. е. описывает все необратимые векторы коммутативной подалгебры третьего типа. Следовательно при некотором целом значении $t \le p-1$ имеем $\mathbf{N}^2 = \alpha^t\mathbf{N} \Rightarrow \mathbf{N}^i = \alpha^{t(i-1)}\mathbf{N}$ и $\omega = p-1$, т. е. все необратимые векторы порождаются умножением вектора $\mathbf{N}$ на всевозможные скаляры.

Умножение вектора $\mathbf{N}$ на обратимый вектор $\mathbf{G}$ рассматриваемой коммутативной подалгебры дает некоторый необратимый вектор, поэтому имеем $\mathbf{NG} = \alpha^u\mathbf{N}$ при некотором $u \le p-1$, т. е. умножение $\mathbf{N}$ на $\mathbf{G}$ эквивалентно умножению $\mathbf{N}$ на некоторый скаляр $\mu = \alpha^u$. Поэтому при задании скрытой циклической группы, генерируемой необратимым вектором $\mathbf{N}$, в схемах ЭЦП [2, 4], основанных на вычислительной трудности СЗДЛ периодическая функция

$$F(i, j) = \mathbf{Y}^i\mathbf{T}\mathbf{Z}^j = \mathbf{A}\mathbf{N}^k\mathbf{B}^{-1} =$$

$$= \mathbf{A}\mu\mathbf{N}\mathbf{B}^{-1} = \mu(\mathbf{A}\mathbf{N}\mathbf{B}^{-1}) = \mu\mathbf{N}',$$

где $\mathbf{Y} = \mathbf{A}\mathbf{N}^x\mathbf{A}^{-1}$, $\mathbf{Z} = \mathbf{B}\mathbf{N}\mathbf{B}^{-1}$ и $\mathbf{T} = \mathbf{A}\mathbf{E}_\mathbf{N}\mathbf{B}^{-1}$ — элементы открытого ключа; $\mathbf{A}$, $\mathbf{N}$ и $\mathbf{B}^{-1}$ — попарно неперестановочные векторы, принимает значения в циклической группе генерируемой некоторым необратимым вектором $\mathbf{N}'$. Это означает, что секретный ключ x может быть вычислен на квантовом компьютере с помощью алгоритма Шора [5].

Модификация схемы ЭЦП [4] со скрытой циклической группой, генерируемой обратимым вектором $\mathbf{G}$, и открытым ключом включающим элементы $\mathbf{Y} = \mathbf{A}\mathbf{G}^x\mathbf{A}^{-1}$, $\mathbf{Z} = \mathbf{B}\,\mathbf{G}\,\mathbf{B}^{-1}$ и

$\mathbf{T}=\mathbf{ANB}^{-1}$ не устраняет данной проблемы, поскольку для указанной периодической функции имеем аналогичную ситуацию:

$$F(i,j) = \mathbf{Y}^i\mathbf{TZ}^j = \mathbf{AG}^k\mathbf{NB}^{-1} =$$
$$= \mathbf{A}\mu'\,\mathbf{NB}^{-1} = \mu'\left(\mathbf{ANB}^{-1}\right) = \mu'\ \mathbf{N}'.$$

Для устранения выявленной проблемы при использовании согласующего элемента открытого ключа вида $\mathbf{T}=\mathbf{AE_NB}^{-1}$ или вида $\mathbf{T}=\mathbf{ANB}^{-1}$ следует задать схему ЭЦП над КНАА размерности 6 или 8, при которой число необратимых элементов в коммутативных алгебрах равно примерно p^2 и имеется возможность выбора в качестве генератора циклической группы необратимого вектора **N**, имеющего значение порядка равное $p^2 - 1$, $p + 1$ или большому простому делителю числа $p + 1$ [7]. Для реализации такой возможности в следующем разделе статьи предлагается унифицированный способ задания КНАА произвольных четных размерностей.

Унифицированный способ задания КНАА четных размерностей

В основу предлагаемого способа задания множества КНАА для размерностей $m = 6$ и $m = 8$ положена формула генерации ТУБВ для произвольных четных размерностей из работы [7]. Для получения возможности задания нескольких различных КНАА для фиксированного значения размерности, в формулу [7] вносится целочисленный параметр $d \in \{0, 1, \ldots, m-1\}$, для различных значений которого задаются различные КНАА для каждого фиксированного значения m, а именно, для четных значений d предлагается следующая модифицированная формула задания ТУБВ:

$$\mathrm{e}_i\mathrm{e}_j = \begin{cases} \mathrm{e}_{i+j+d \bmod m} \ (i \bmod 2 = 0); \\ \mathrm{e}_{i-j-d \bmod m} \ (i \bmod 2 = 1,\ \ j \bmod 2 = 0); \\ \lambda\mathrm{e}_{i-j-d \bmod m} \ (i \bmod 2 = 1,\ j \bmod 2 = 1). \end{cases} \quad (4)$$

Для фиксированного значения m для нечетных значений d предлагается следующая формула задания ТУБВ:

$$\mathrm{e}_i\mathrm{e}_j = \begin{cases} \mathrm{e}_{i-j-d \bmod m} \ (i \bmod 2 = 0,\ \ j \bmod 2 = 1); \\ \lambda\mathrm{e}_{i-j-d \bmod m} \ (i \bmod 2 = 0,\ j \bmod 2 = 0); \\ \mathrm{e}_{i+j+d \bmod m} \ (i \bmod 2 = 1). \end{cases} \quad (5)$$

Доказательство того, что формулы (4) и (5) генерирует ТУБВ, задающие ассоциативное умножение векторов для произвольных четных размерностей $m > 2$ выполняется аналогично доказательству выполненному в работе [7]. Для значения размерности $m = 6$ формула (4) задает две различные алгебры, а формула (5) — три. Для $m = 8$ формула (4) задает три различные алгебры, а формула (5) — четыре. Вид вектора, являющегося глобальной двухсторонней единицей алгебры, зависит от значения параметра d (см. табл. 5 для случая $m = 6$). Примеры генерируемых ТУБВ представлены в табл. 6 ($d = 2$) и табл. 7 ($d = 4$).

Таблица 5

Виды глобальных двухсторонних единиц E в шестимерных КНАА

Формула, задающая ТУБВ	Значение d	Единичный вектор **E**
(4) [7]	0	(1,0,0,0,0,0)
(5)	1	(0,1,0,0,0,0)
(4)	2	(0,0,1,0,0,0)
(5)	3	(0,0,0,1,0,0)
(4)	4	(0,0,0,0,1,0)
(5)	5	(0,0,0,0,0,1)

Таблица 6

Задание шестимерной КНАА ($\lambda \neq 0$) с глобальной единицей (0,0,0,0,1,0)

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_5$	$\lambda\,\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\,\mathbf{e}_2$	$\mathbf{e}_1$	$\lambda\,\mathbf{e}_0$
$\mathbf{e}_2$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\mathbf{e}_1$	$\lambda\,\mathbf{e}_0$	$\mathbf{e}_5$	$\lambda\,\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\,\mathbf{e}_2$
$\mathbf{e}_4$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_5$	$\mathbf{e}_3$	$\lambda\,\mathbf{e}_2$	$\mathbf{e}_1$	$\lambda\,\mathbf{e}_0$	$\mathbf{e}_5$	$\lambda\,\mathbf{e}_4$

Таблица 7

Задание восьмимерной КНАА ($\lambda \neq 0$) с глобальной единицей (0,0,0,0,1,0,0,0)

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

Выполнение вычислительных экспериментов подтвердило ожидание того, что во всех шестимерных и восьмимерных КНАА, заданных по формулам (4) и (5), при значении структурного коэффициента λ, являющегося квадратичным невычетом по модулю простого числа p, содержатся необратимые элементы, порядок которых равен значению $p^2 - 1$.

Например, в алгебре, заданной по табл. 6 при $p = 23$, $\lambda = 11$ (квадратичный невычет по модулю 23), необратимый вектор $\mathbf{N} = (13,18,17,15,17,22)$ генерирует циклическую группу порядка $\Omega = p^2 - 1 = 528$ с единичным элементом, равным

$$\mathbf{E_N} == (15, 21, 16, 3, 16, 22).$$

В алгебре, заданной по табл. 6 при $p = 257$, $\lambda = 13$ (квадратичный вычет по модулю 257), необратимый вектор

$$\mathbf{N} = (13, 151, 134, 113, 211, 123, 156, 145)$$

генерирует циклическую группу порядка $\Omega = p^2 - 1 = 66048$, содержащую единицу в виде необратимого вектора

$$\mathbf{E_N} = (32, 109, 225, 148, 33, 109, 225, 148).$$

Представляет интерес рассмотрение строения коммутативных подалгебр, содержащихся в этих шестимерных и восьмимерных некоммутативных алгебрах. Изучение этого вопроса может быть осуществлено методом вычисления подмножества элементов, взаимно перестановочных с заданным элементом, аналогично тому, как это сделано для случая четырехмерных алгебр, задаваемых по прореженным табл. 1–4. Однако такое исследование представляется самостоятельной задачей, имеющей более высокую трудность, связанную с необходимостью исследования решений систем из шести и восьми линейных уравнений.

Можно ожидать, что для случаев размерностей $m = 6$ и $m = 8$ КНАА других типов также будут содержать обратимые векторы, генерирующие циклические группы порядка $\Omega = p^2 - 1$, т. е. для реализации схем ЭЦП и схем открытого согласования ключа, основанны на скрытой задаче дискретного логарифмирования и использующие скрытые группы, генерируемые необратимым элементом, могут оказаться пригодными шестимерные и восьмимерные алгебры и других типов.

Например, в алгебре, заданной по табл. 8 при $p = 23$, $\lambda = 11$, необратимый вектор $\mathbf{N} = (13, 12, 12, 15, 13, 22)$ генерирует циклическую группу порядка $\Omega = 176$ (делитель числа $p^2 - 1$) с единицей, равной $\mathbf{E_N} = (16, 4, 4, 3, 2, 18)$. Необратимый вектор $\mathbf{N} = (14, 15, 10, 11, 10, 19)$ генерирует циклическую группу порядка $\Omega = p^2 - 1 = 528$ с единицей, равной $\mathbf{E_N} = (16, 1, 7, 12, 4, 7)$.

Таблица 8

Задание шестимерной КНАА ($\lambda \neq 0$) с глобальной единицей (1,0,0,0,0,0)

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_5$	$\mathbf{e}_3$	$\mathbf{e}_4$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$
$\mathbf{e}_5$	$\mathbf{e}_5$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_0$

Обсуждение

Установлено типовое строение ряда четырехмерных КНАА с глобальной двухсторонней единицей, задаваемых по прореженным ТУБВ. Показано, что каждая из них разбивается на множество коммутативных подалгебр порядка p^2, включающих мультипликативную группу одного из трех типов. Все подалгебры попарно пересекаются в множестве скалярных векторов. Количество подалгебр каждого типа задается формулами (1), (2) и (3). Видно, что КНАА, заданные по табл. 3, при значении $\lambda = 1$ описывают алгебру матриц размерности 2×2. Таким образом, установленные ограничения на использование четырехмерных алгебр в криптосхемах, основанных на СЗДЛ и использующих необратимые векторы для генерации параметров открытого ключа, относятся также и к алгебре матриц 2×2.

Для реализации указанных криптосхем предложено использование шестимерных и восьмимерных КНАА в качестве алгебраического носителя. Разработана унифицированная формула генерации расширенного подкласса КНАА четных размерностей. Показано, что шестимерные и восьмимерные алгебры из этого подкласса включают необратимые векторы, генерирующие циклические группы порядка $p^2 - 1$, что устраняет ограничения, возникающие при использовании четырехмерных КНАА. Продемонстрировано, что и другие типы шестимерных алгебр обладают указанным свойством, т. е. выбор в качестве алгебраического носителя криптосхем, основанных на СЗДЛ, шестимерных и восьмимерных алгебр является предпочтительным по сравнению с использованием четырехмерных КНАА.

Таким образом, в предложенных ранее в схемах ЭЦП [2—4] целесообразно перейти от использования четырехмерных КНАА к использованию шестимерных и восьмимерных некоммутативных алгебр с глобальной единицей.

Заключение

Показана необходимость увеличения размерности КНАА, используемых в качестве алгебраического носителя схем ЭЦП, использующих скрытую циклическую группу, генерируемую необратимым вектором, до значений $m = 6$ и $m = 8$. При этом шестимерные КНАА представляются предпочтительными с точки зрения получения более высокой производительности и меньших размеров открытого ключа по сравнению со случаем использования восьмимерных алгебр. При разработке конкретных алгоритмов ЭЦП важной является информация о строении коммутативных подалгебр, содержащихся в КНАА, однако для каждой конкретной КНАА размерностей $m = 6$ и $m = 8$ изучение этого вопроса составляет задачу самостоятельного исследования.

Работа выполнена при частичной финансовой поддержке РФФИ (проект № 21-57-54001-Вьет_а) и бюджетной темы № 0060-2019-0010.

Литература

1. *Moldovyan N. A., Moldovyan A. A.* Finite Noncommutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem // Вестник ЮУрГУ. Сер. "Математическое моделирование и программирование". 2019. Т. 12. № 1. С. 66—81.

2. *Молдовян Н. А., Абросимов И. К.* Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23—32.

3. *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.

4. *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.

5. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. *SIAM Journal of Computing.* 1997. V. 26. P. 1484—1509.

6. *Moldovyan D. N.* New Form of the Hidden Logarithm Problem and Its Algebraic Support // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. № 2 (93). P. 3—10.

7. *Moldovyan N. A.* Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // Quasigroups and Related Systems. 2018. V. 26. №. 2. P. 263—270.

Setting six-dimensional algebras as supports of the signature schemes based on the hidden discrete logarithm problem

D. N. Moldovyan
St. Petersburg Federal Research Centerof of the RAS (SPC RAS), St. Petersburg, Russia

The structure of a number of four-dimensional finite non-commutative associative algebras is considered and some problems are shown with the use of non-invertible elements of such algebras as parameters of digital signature schemes based on the hidden discrete logarithm problem. To eliminate these problems, the use of six-dimensional and eight-dimensional algebras is proposed. A unified method for specifying algebras of the latter types has been developed.

Keywords: information security, post-quantum cryptography, digital signature, finite associative algebra, commutative algebra, multiplicative group.

Bibliography — 7 references. *Received February 22, 2021*

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004.056

DOI: 10.52190/2073-2600_2021_1_33

Адаптация метода биометрической идентификации по голосу к тихому произнесению парольных фраз для противодействия акустической речевой разведке

Р. А. Васильев, канд. техн. наук
АО «Финансы, Информация, Технология» (АО «ФИНТЕХ»), Москва, Россия

Рассмотрены особенности биометрической идентификации по голосу (БИГ) при условии тихого произнесения парольных фраз (ТПФ). Предложен адаптированный к ТПФ метод БИГ, основанный на применении метода обеляющего фильтра (МОФ). Описана программная реализация предложенного метода — Информационная система идентификации дикторов по голосу (ИС ИДГ), позволяющая проводить БИГ при условии ТПФ для противодействия акустической речевой разведке (АРР).

Ключевые слова: биометрическая идентификация по голосу, метод обеляющего фильтра, акустическая речевая разведка.

Многие финансовые операции, идентификация в системах разграничения доступа, запросы конфиденциальной информации по телефону, управление различными устройствами основаны на применении систем БИГ [1].

БИГ существенно отличается от стандартных систем идентификации и систем контроля управления доступом, использующих символьные пароли и ключи. БИГ производится по уникальным, индивидуальным признакам личности и практически исключает вероятность несанкционированных действий, связанных с потерей, кражей или передачей пароля третьим лицам [2].

Широкое применение БИГ-систем влечет за собой повышенный интерес со стороны злоумышленников. Наиболее частыми являются атаки с использованием ранее применяемых биометрических признаков (например, аудио-запись парольной фразы).

Системы БИГ необходимо проектировать так, чтобы свести к минимуму указанные атаки. В данной статье описан адаптированный к ТПФ метод БИГ, основанный на применении МОФ, реализованный в ИС ИДГ [3], доработанной для решения задачи защиты речевой информации (парольные фразы) от утечки по акустическим каналам [4].

Метод обеляющего фильтра

Общая формулировка задачи БИГ сводится к тому, что требуется отнести выборку из речи пользователя X к одному из $R > 1$ образов речи пользователей, хранящихся в голосовой базе [5]. Каждому образу соответствуют образцы речи конкретного пользователя, обладающие общими признаками, образующими образ голоса пользователя (ОГП). Каждый ОГП обладает определенным набором устойчивых признаков P_r, $r = \overline{1, R}$. В данном случае решение

Васильев Роман Александрович, заместитель начальника отдела внедрения и сопровождения решений по защите информации Департамента информационной безопасности.
E-mail: r.vasilev@fintech.ru

Статья поступила в редакцию 15 февраля 2021 г.

задачи БИГ сводится к установлению соотношения

$$P_X = P_v,\ v \le R \qquad (1)$$

между набором признаков пользователя X и одним из ОГП в базе голосовых данных.

Проще всего поставленная задача решается в параметрическом варианте, когда каждое распределение P_r, $r = \overline{1,R}$, берется из некоторого параметрического семейства. Например, это может быть семейство n-мерных нормальных (гауссовских) законов $P_{_0 r} = N(K_r)$, определенных на множестве допустимых значений всех элементов $(n \times n)$-матрицы автоковариаций K_r, $r = \overline{1,R}$ (в данном случае предполагается, что все используемые сигналы заранее центрированы). Восстановление закона $N(K_r)$ по обучающей выборке X_r сводится к элементарной процедуре статистического оценивания его неизвестной автоковариационной матрицы (АКМ) по формуле

$$K_r = \frac{1}{L}\sum_{l=1}^{L} \mathbf{x}_l \overset{\mathrm{T}}{\mathbf{x}}_l, \qquad (2)$$

где индексом "T" обозначена операция транспонирования векторов;

L — число независимых образцов речи в пределах r-го распределения P_r;

$\overset{(r)}{\mathbf{x}}_l$ — n-вектор-столбец с координатами из R^n.

Задача (1) после этого формулируется как проверка R простых гипотез о неизвестном законе распределения:

$$H_r : P_X = N(K_r),\ \ r \in \overline{1,R}. \qquad (3)$$

Это стандартная задача статистической классификации. Ее решение обычно основывается на критерии максимального правдоподобия. Применительно к предложенной модели речевых сигналов в виде L независимых отрезков (массивов) длиной n отсчетов каждый такая задача подробно рассмотрена в работе [6]. Показано, что оптимальный алгоритм принятия решения по выборке $X = \{\mathbf{x}_l\}$, $l = \overline{1,L}$, основывается на достаточной статистике общего вида:

$$\lambda_r(X) = \mathrm{tr}[K_X K_r^{-1}] + \ln|K_r|,\ \ r = \overline{1,R}, \qquad (4)$$

где K_X — выборочная оценка АКМ наблюдений по формуле (2); символами tr (…) и |…| обозначены, соответственно, след и определитель квадратных (n×n)-матриц.

Решение принимается в пользу гипотезы H_v из (1), если соответствующая ей v-я статистика (4) принимает минимальное значение из R рассматриваемых альтернатив.

Указанный алгоритм в асимптотическом варианте (при $n \to \infty$) для несингулярного случая, когда $\lim|K_r| \ne 0$, может быть переписан следующим образом [7]:

$$\lambda_r(X) = \frac{\sigma_r^2(X)}{\sigma_r^2} + \ln\sigma_r^2,\ \ r = \overline{1,R}, \qquad (5а)$$

$$\sigma_r^2(X) = \frac{1}{L}\sum_{l=1}^{L}\left[y_l^{(r)}(X)\right]^2;$$

$$y_l^{(r)}(X) = \overset{\mathrm{T}}{\mathbf{a}}_r \mathbf{x}_l, \qquad (5б)$$

$$\mathbf{a}_r = \sigma_r^2 K_r^{-1}\boldsymbol{\Gamma},\quad \sigma_r^2 = \left[\overset{\mathrm{T}}{\boldsymbol{\Gamma}} K_r^{-1}\boldsymbol{\Gamma}\right]^{-1},$$

где $\boldsymbol{\Gamma} = \mathrm{col}_n(1, 0, ..., 0)$ — n-вектор-столбец, составленный из нулей за исключением единицы на первой позиции. Решение здесь принимается в пользу гипотезы H_v при условии минимизации взвешенной с коэффициентом $1/\sigma_v^2$ и смещенной на $\ln\sigma_v^2$ величины выборочной дисперсии $\sigma_v^2(X)$ отклика на сигнал X декоррелятора v-го канала (5б). Структура такого декоррелятора однозначно определяется вектором коэффициентов линейной авторегрессии (АР-коэффициентов) $\mathbf{a}_v$, $v \le R$. Это стандартная формулировка МОФ в задачах распознавания образов [8].

Главная идея метода состоит в существенной (в десятки раз) редукции (или сжатии данных) за счет того, что в базе априорных данных хранятся не сами отрезки речи длиной $nL = 10^2$—10^3 отсчетов каждый, а их образы в виде набора из R векторов АР-коэффициентов (их также часто называют коэффициентами

линейного предсказания, КЛП), размерность которых $M = 10—30 < nL$ в реальных условиях ограничивается конечной степенью сложности спектрального состава человеческого голоса. При этом в отличие от известных алгоритмов автоматического распознавания речи на основе КЛП [9] в рассматриваемом МОФ применяется принципиально иной критерий для оценивания рассогласования между различными речевыми образами, уходящий своими корнями в теоретико-информационный подход и информационную метрику Кульбака—Лейблера [10].

Программа экспериментальных исследований

Для экспериментальных исследований использовали ранее разработанную и проверенную ИС ИДГ [11, 12], адаптированная к ТПФ посредством доработки модуля регулировки чувствительности к уровню речевого сигнала пользователя (диктора) *X*.

Главное окно ИС ИДГ представлено на рис. 1.

Экспериментальные исследования состоят из трех этапов (табл. 1).

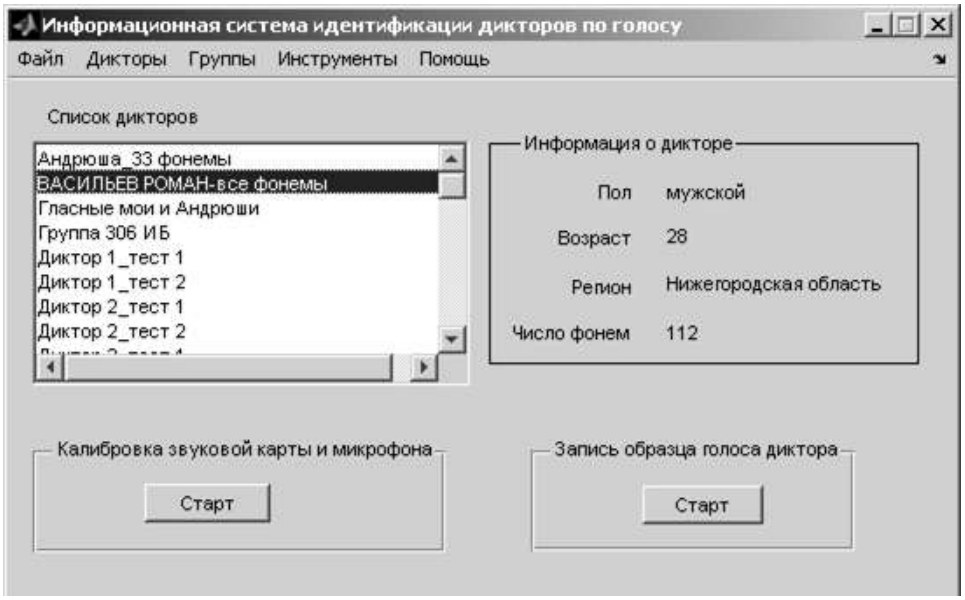


Рис. 1. Главное окно программы ИС ИДГ

Таблица 1

Этапы экспериментальных исследований

Номер эксперимента	Цель	Задачи
1	Выявление эталонного уровня сигнала речевой идентификации пользователя по голосу, анализ недостатков и преимуществ сигналов разного уровня в системе голосовой идентификации	Запись в БД эталонного уровня сигнала для дальнейших экспериментов, выявление среднего, низкого и высокого уровней сигнала для голосовой идентификации, определение оптимального уровня сигнала для голосовой идентификации на основе преимуществ и недостатков различного уровня сигнала
2	Определение вероятности правильной идентификации пользователей по голосу	Определение вероятности правильной идентификации трех пользователей по голосу при условии разделения уровня сигнала на 3 интервала (до 20 дБ, от 25—35 дБ, более 40 дБ)
3	Определение октавных коэффициентов звукоизоляции в типовом помещении, определение того, выполняются ли нормы защищенности в данном помещении для работы с конфиденциальной информацией	Определение назначения объекта контроля, выбор требуемого уровня защиты от утечки речевой информации по акустическим каналам. Определение контролируемой зоны, смежных помещений и ограждающих конструкций, контрольных точек для замера уровня акустического сигнала (шума). Проверка выполнения норм защищенности от АРР

В первом эксперименте, для выявления эталонного уровня сигнала *Uc* для речевой идентификации пользователя, проведено 9 опытов с различным уровнем сигнала (от 10 до 55 дБ). В процессе опытов уровни сигналов разбиты на 3 группы: высокие (*Uc* ~ 40—55 дБ, обычная повседневная речь), средние (*Uc* ~ 25—35 дБ, шепот человека) и низкие (*Uc* ~ 10—20 дБ, едва слышный шепот).

Проведен анализ каждой из групп сигналов. Определена вероятность идентификации пользователя по голосу (табл. 2).

На рис. 2 показана успешная идентификация по голосу в ИС ИДГ.

Далее представлен случай с неуспешной идентификацией по голосу в ИС ИДГ (рис. 3).

Выводы по первому эксперименту.

- Определен уровень эталонного сигнала речевой идентификации *Uc* = 30 дБ.
- Сигналы от 10—20 дБ воспринимаются ИС ИДГ гораздо хуже, в связи с чем процент успешной голосовой идентификации очень мал, но преимуществом тихого воспроизведения парольных фраз является отсутствие акустического канала утечки информации.
- Сигналы от 25—35 дБ ИС ИДГ воспринимает гораздо лучше, нежели сигналы от 10—20 дБ, как следствие, процент успешной идентификации оказывается выше и достигает более 70 %, однако вероятность утечки речевой информации возрастает и необходимо проводить дополнительную оценку защищенности по акустическим каналам.
- Сигналы от 40—55 дБ ИС ИДГ воспринимает лучше, чем сигналы двух других групп, и процент успешной идентификации пользователя по голосу достигает более 90 %. Несмотря на высокий процент успешной идентификации, этой группе сигналов присуща высокая вероятность утечки речевой информации по акустическим каналам.

Таблица 2

Вероятность идентификации пользователя по голосу

Уровень сигнала *Uc*, дБ	Вероятность идентификации	Вывод
~ 40—55	Более 90 %	Идентификация в 90 % проходит успешно, но вероятность утечки информации по акустическому каналу высока
~ 25—35	Более 70 %	Идентификация в более 70 % проходит успешно, вероятность утечки информации по акустическому каналу в пределах нормы
~ 10—20	Менее 50 %	Идентификация проходит неуспешно, вероятность утечки информации по акустическому каналу ничтожно мала

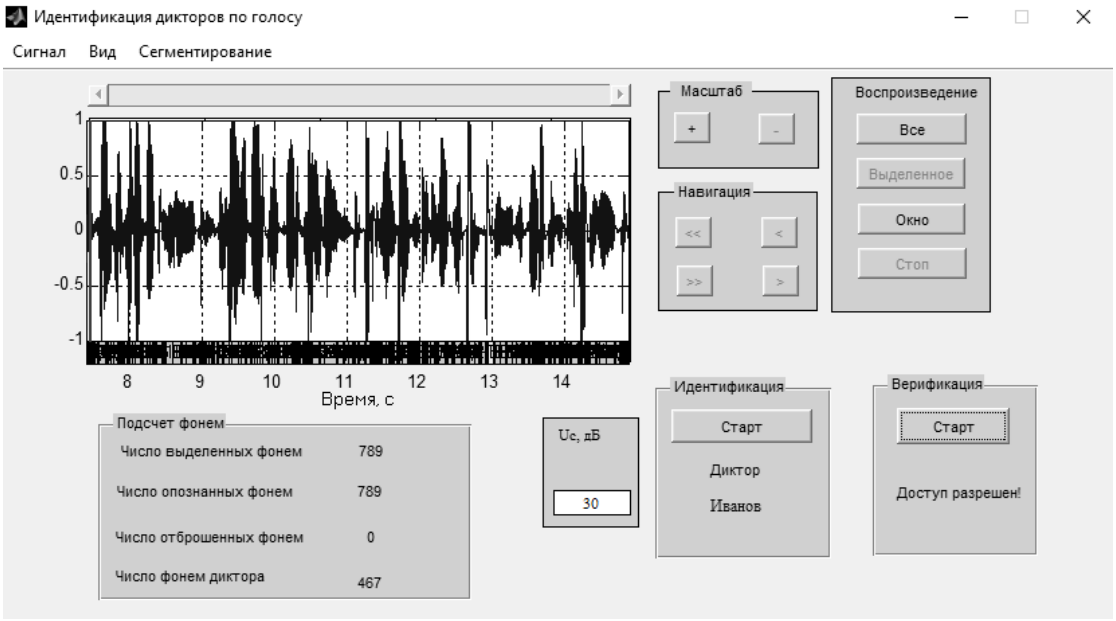


Рис. 2. Успешная идентификация по голосу при Uc=30 дБ

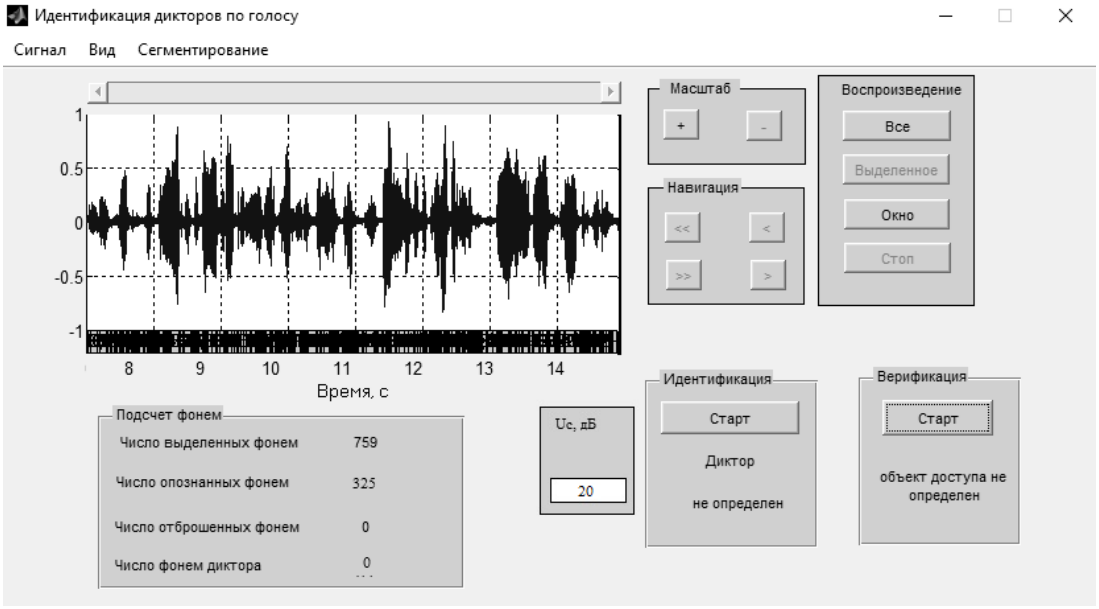


Рис. 3. Неуспешная идентификация по голосу при Uc = 20 дБ

Во втором эксперименте определена вероятность правильной идентификации трёх пользователей (Иванов, Петров, Сидоров) по голосу при условии разделения уровня сигнала для каждого из пользователей на 3 интервала: до 20 дБ, 25—35 дБ, более 40 дБ (табл. 3).

Рассмотрим каждый из трех диапазонов отдельно. Анализируя 1-й диапазон (*Uc* более 40 дБ), можно сказать, что идентификация пользователей по голосу проходит во всех случаях успешно. Средний уровень сигнала для пользователя Иванов равен 47,5 дБ, идентификация проходит успешно во всех опытах. Средний уровень сигнала для пользователя Петров 46,5 дБ, идентификация проходит успешно во всех опытах. Пользователь Сидоров имеет средний уровень голосового сигнала 47 дБ, для которого идентификация во всех опытах также проходит успешно.

При проведении анализа 2-го диапазона (*Uc* ~ 25—35 дБ) средний уровень сигнала для пользователя Иванов равен 31 дБ, идентификация в 4 опытах успешно завершена. Пользователь Петров имеет уровень сигнала 30,75 дБ, идентификация во всех опытах прошла успешно. Что касается пользователя Сидорова, то его средний уровень сигнала составляет 29 дБ, как следствие, из четырех экспериментов в двух идентификация проходит успешно, а в двух — программа не может распознать голос.

Таблица 3

Вероятность правильной идентификации трёх пользователей

ФИО	Uc_1, дБ	Uc_2, дБ	Uc_3, дБ	Uc_4, дБ	$U_{ср}$, дБ	Идентификация прошла успешно			
						P_1	P_2	P_3	P_4
Uc более 40 дБ									
Иванов	40	45	50	55	47,5	Да	Да	Да	Да
Петров	54	43	48	41	46,5	Да	Да	Да	Да
Сидоров	49	41	52	46	47	Да	Да	Да	Да
Uc ~ 25—35 дБ									
Иванов	29	30	31	34	31	Да	Да	Да	Да
Петров	28	34	31	30	30,75	Да	Да	Да	Да
Сидоров	25	30	26	35	29	Нет	Да	Нет	Да
Uc ~ до 20 Дб									
Иванов	12	20	15	17	16	Нет	Нет	Нет	Нет
Петров	15	17	19	20	17,75	Нет	Нет	Нет	Нет
Сидоров	18	14	19	17	17	Нет	Нет	Нет	Нет

В 3-ем диапазоне (*Uc* до 20 дБ) для трех пользователей системы уровень голосового сигнала каждого из них приблизительно равен 17 дБ. Вероятность идентификации для пользователей с таким низким уровнем сигнала стремится к нулю.

Выводы по второму эксперименту.

- Выбрав в 1-м опыте эталонный уровень сигнала *U*эс = 30 дБ, определяем, что идентификация пользователя по голосу проходит только тогда, когда уровень голосового сигнала пользователя *Uc* > 26 дБ.
- Уровень сигнала более 40 дБ во всех опытах проходит идентификацию, но вероятность утечки информации по акустическим каналам возрастает с увеличением *Uc*.
- Оптимальным уровнем сигнала для успешной идентификации пользователя по голосу в ИС ИДГ является *Uc* = 27—33 дБ.

В соответствии с методикой [13] в *третьем эксперименте* проведена оценка защищенности речевой информации (парольные фразы) от утечки по акустическим каналам в типовом офисном помещении (ТОП) с помощью системы оценки защищенности выделенных помещений по виброакустическому каналу "ШЕПОТ" (сертификат ФСТЭК № 643 от 05.07.2002).

Границей контролируемой зоны ТОП являются его наружные и внутренние стены, а также перекрытие пола и потолка.

В результате анализа возможных каналов утечки речевой информации, инженерно-строительных и организационно-режимных мер, применяемых в ТОП, произведен расчет значений октавных коэффициентов звукоизоляции ограждающих конструкций Q_i в выбранных контрольных точках (КТ) (табл. 4).

Таблица 4

Оценка защищенности ТОП

Номер октавной полосы *i*	Измеренный уровень акустического (вибрационного) шума в контрольной точке $L_{шi}$ ($V_{шi}$), дБ	Уровень измеренного суммарного акустического (вибрационного) сигнала и акустического (вибрационного) шума в КТ $L_{(с+ш)i}$ ($V_{(с+ш)i}$), дБ	Расчетный уровень измеренного акустического (вибрационного) сигнала в контрольной точке $L_{с2i}$ ($V_{с2i}$), дБ	Октавные уровни звукоизоляции (виброизоляции) в контрольной точке Q_i (G_i), дБ	Выполнение норм
Контрольная точка № 1 — стена с дверным проемом между ТОП и коридором					
1	22,00	32,10	10,10	44,00	Вып.
2	21,10	30,70	8,60	44,80	Вып.
3	21,30	29,20	6,90	48,90	Вып.
4	21,90	34,50	12,60	44,50	Вып.
5	25,20	30,20	3,00	51,60	Вып.
Контрольная точка № 2 — стена между ТОП и гардеробом (смежные помещения)					
1	20,20	28,50	7,30	47,90	Вып.
2	21,80	27,60	3,80	51,30	Вып.
3	20,80	27,00	5,20	52,40	Вып.
4	22,70	29,60	5,90	54,00	Вып.
5	21,00	29,80	7,80	49,70	Вып.
Контрольная точка № 3 — окно (улица)					
1	25,20	35,60	10,40	44,80	Вып.
2	25,40	36,60	11,20	43,90	Вып.
3	21,40	29,10	6,70	50,90	Вып.
4	27,20	38,70	11,50	48,40	Вып.
5	29,90	35,30	3,40	54,10	Вып.
Контрольная точка № 4 — перекрытие пола					
1	21,40	29,20	6,80	47,60	Вып.
2	19,10	25,80	5,70	49,40	Вып.
3	19,20	28,90	8,70	49,10	Вып.
4	20,40	27,50	6,10	53,80	Вып.
5	22,20	29,10	5,90	52,40	Вып.
Контрольная точка № 5 — перекрытие потолка					
1	21,70	28,30	5,60	50,20	Вып.
2	19,00	26,20	6,20	49,80	Вып.
3	19,10	27,80	7,70	51,10	Вып.
4	20,20	27,80	6,60	54,20	Вып.
5	21,80	28,30	5,50	53,90	Вып.

Вывод по третьему эксперименту.

В результате проведенных измерений и расчетов установлено, что при среднем уровне сигнала в 30 дБ значения октавных коэффициентов звукоизоляции ограждающих конструкций и инженерно-технических систем во всех контрольных точках соответствуют нормативным [13], что обеспечивает защищённость данного ТОП от утечки речевой конфиденциальной информации по акустическому каналу.

Заключение

Рассмотрены особенности БИГ при условии ТПФ, выявлен оптимальный уровень сигнала *U*с ~ 30 дБ для адаптации метода идентификации в ИС ИДГ, что позволило получить высокую вероятность правильной БИГ по сравнению с другим методом [14]. С учетом эталонного уровня сигнала сделаны замеры октавных коэффициентов звукоизоляции для ТОП и установлено, что при уровне сигнала *Uc* ~ 30 дБ утечки речевой информации по акустическим каналам не происходит.

Литература

1. *Николаев Д. Б., Васильев Р. А.* Анализ возможности применения голосовой идентификации в системах разграничения доступа к информации // Научный результат. Сер. "Информационные технологии". 2016. Вып. 1. С. 48—57.
2. *Савченко В. В., Васильев Р. А.* Анализ эмоционального состояния дикторов по голосу на основе фонетического детектора лжи // Научные ведомости Белгородского государственного университета. 2014. Вып. № 21(192)32/1. С. 186—195.
3. *Васильев Р. А.* Свид. о гос. регистрации программы для ЭВМ № 2015663306. Программа идентификации дикторов по голосу. — М.: Роспатент, 2015.
4. *Бузов Г. А.* Защита от утечки информации по техническим каналам. — М., 2005.
5. *Цыпкин Я. З.* Адаптация и обучение в автоматических системах. — М.: Наука, 1968.
6. *Савченко В. В.* Информационная теория восприятия речи // Изв. вузов России. Радиоэлектроника. 2007. Вып. 6. С. 3—9.
7. *Савченко В. В.* Теоретико-информационное обоснование гауссовой модели сигналов в задачах автоматического распознавания речи // Изв. вузов России. Радиоэлектроника. 2008. Вып. 1. С. 24—33.
8. *Савченко В. В., Акатьев Д. Ю., Карпов Н. В.* Автоматическое распознавание элементарных речевых единиц методом обеляющего фильтра // Изв. вузов России. Радиоэлектроника. 2007. Вып. 4. С. 11—19.
9. *Потапова Р. К.* Речь: коммуникация, информация, кибернетика: учеб. пособие. Изд. 2. — М.: Эдиториал УРСС, 2001.
10. *Кульбак С.* Теория информации и статистика. — М.: Наука, 1967.
11. *Васильев Р. А.* Биометрическая идентификация пользователей информационных систем на основе кластерной модели элементарных речевых единиц: дисс. … канд. тех. наук. — М., 2017. — 153 с.
12. *Васильев Р. А.* Исследование фонетического строя речи и идентификация дикторов по голосу // Вопросы защиты информации. 2013. № 1(100). С. 43—51.
13. *Волобуев С. В.* Оценка акустической защищенности с применением инструментальных средств // Системы безопасности связи и телекоммуникаций. 1999. № 25. С. 38—45.
14. *Аграновский А. В., Леднов Д. А.* Метод текстонезависимой идентификации пользователя на основе индивидуальности произношения гласных звуков // Акустика и прикладная лингвистика: Ежегодник РАО. 2002. Вып. 3. С. 103—115.

Adaptation of the biometric voice identification method to the quiet pronunciation of passphrases to counteract acoustic speech intelligence

R. A. Vasiliev

Joint Stock Company "Finance, Information, Technology" (JSC "FINTECH"), Moscow, Russia

The features of biometric voice identification (BIG) under the condition of silent pronunciation of password phrases (TPF) are considered. The BIG method adapted to TPF, based on the application of the whitening filter method (WHF), is proposed. Described is the software implementation of the proposed method — "Information system for identifying speakers by voice" (IS IDG), which makes it possible to carry out BIG under the condition of TPF to counteract acoustic speech reconnaissance (APP).

Keywords: biometric voice identification, whitening filter method, acoustic speech intelligence.

Bibliography — 14 references. *Received February 15, 2021*

УДК 004.056.5

DOI: 10.52190/2073-2600_2021_1_40

Использование нейронных сетей для обеспечения защиты информации на режимных объектах организаций и 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

Рассмотрена возможность применения систем идентификации личности и защиты информации, реализуемых с помощью нейронных сетей и элементов искусственного интеллекта.

Ключевые слова: информационная безопасность, нейронные сети, перцептрон, искусственный интеллект.

Для обеспечения задач информационной безопасности, в частности на режимных объектах, при организации контроля доступа, а также защиты от сетевых программных вторжений необходимо использовать системы идентификации личности как в физическом смысле, так и в качестве пользователя информационной системы организации (учреждения).

Системы, имеющие в своем составе арсенал аппаратно-программных средств, повсеместно применяют для задач биометрической идентификации, слежения за поведением программ, находящихся в рамках ресурсов операционных систем. Проблема состоит в сложности описания подобных структур, в выборе математического и программного обеспечения.

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 9 февраля 2021 г.

На практике реализация методов сличения или распознавания образов возможна при применении нейронных сетей, т. е. систем "компьютерного обучения", включающих элементы искусственного интеллекта. С этой точки зрения нейронная сеть представляет собой частный случай методов распознавания образов, дискриминантного анализа, методов кластеризации. Со стороны математического обеспечения процесс обучения нейронных сетей представляется в виде задачи нелинейной оптимизации нескольких параметров [1].

При постановке задачи с применением искусственной нейронной сети следует прежде всего спроектировать структуру сети, а затем построить адекватную модель. При проектировании нейронной сети необходимо решить вопрос о числе слоев и нейронов в каждом слое, а также определить необходимые связи между слоями [2].

Подбор числа нейронов во входном слое обусловлен размерностью входного вектора входных данных. Вместе с тем количество нейронов на выходе принимается равным размерности эталонного набора (вектора) значений, с которыми происходит сравнение.

Примером может служить использование однослойной нейронной сети для анализа уязвимостей в информационной системе (рис. 1).

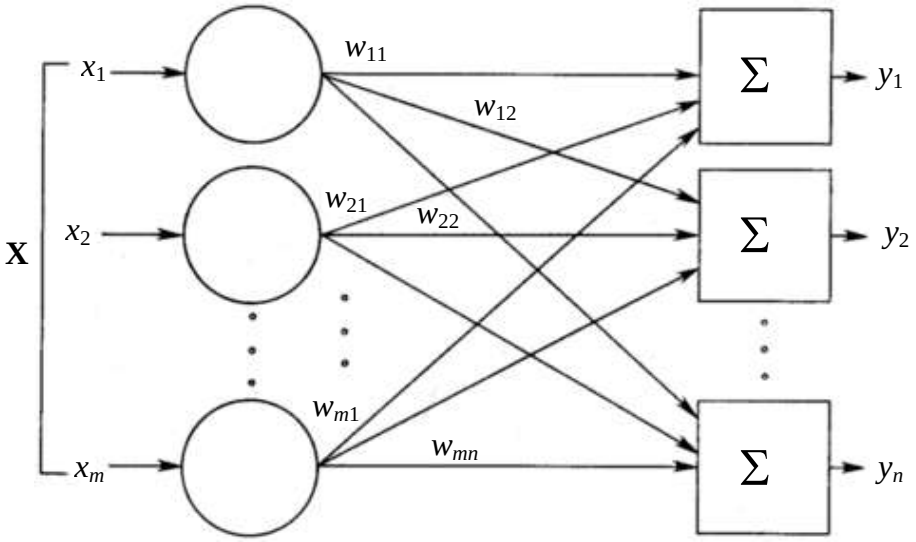


Рис. 1. Однослойная нейронная сеть

Здесь приняты следующие обозначения:

- значения на входе представлены вектором **X**:

$$\mathbf{X}_i = \{x_1, x_2, \ldots, x_m\}; \quad (1)$$

- результат на выходе представлен вектором **Y**:

$$\mathbf{Y}_j = \{y_1, y_2, \ldots, y_n\}; \quad (2)$$

- коэффициенты связи

$$w_{1,i} = \{w_{1,1}, w_{1,2}, \ldots, w_{1,m}\},$$
$$w_{j,1} = \{w_{j,1}, w_{j,2}, \ldots, w_{n,m}\}. \quad (3)$$

Подбор оптимальных значений в (3) является основной задачей, которая реализуется с помощью элементарного аппарата — персептрона — в процессе его "обучения". Эта способность нейронных сетей и будет преимуществом перед алгоритмами, которые реализуются по шаговому принципу "сверху-вниз". Таким образом, задача будет состоять не в трассировке заданной программы, а в нахождении оптимальных коэффициентов связи между нейронами.

Возьмем в качестве примера модель перцептрона, обеспечивающую отнесение объекта к одному из двух заданных классов (рис. 2).

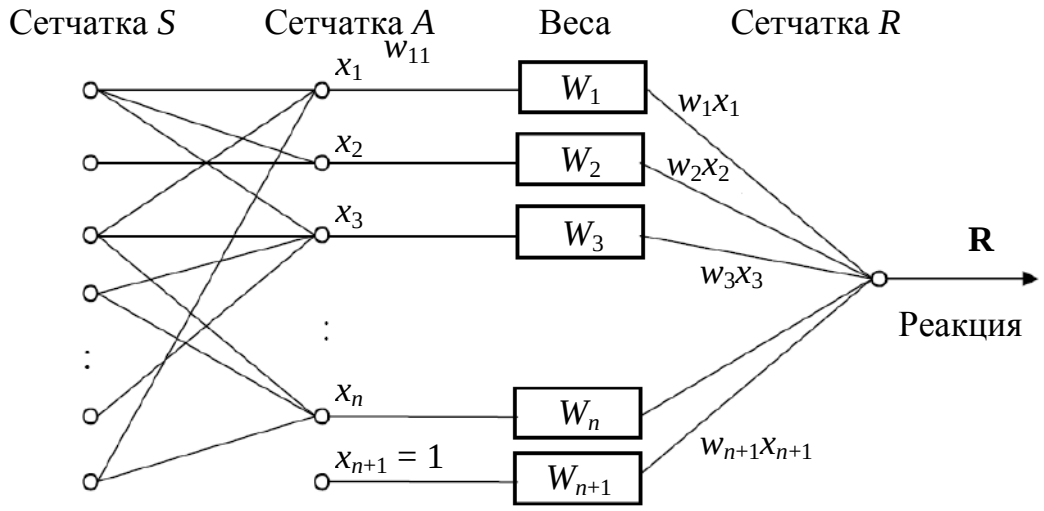


Рис. 2. Структура перцептрона для выборки объектов

Мысленно разобьем структуру. На входе измерительные элементы (сенсоры) сетчатки *S* случайным образом связаны с сенсорами сетчатки *A*. Измерительные элементы, соединенные с его входом, испытывают воздействие извне. При отклонении от пороговых значений сенсоры посылают сигнал на реагирующий элемент *R*. При этом по схеме сигналы суммируются с весовыми коэффициентами. Математическое описание процесса выглядит следующим образом:

$$R(x) = \sum_{i=0}^{n} w_i x_i = (w_i x_i) > 0. \qquad (4)$$

Заключение

В заключение отметим, что при организации обучения перцептрона появляется возможность смоделировать систему отсеивания образов, например фотографий сотрудников, не имеющих нужной степени допуска (в частности, на режимных объектах уголовно-исполнительной системы это обеспечение надзора за осужденными). Внедрение элементов искусственного интеллекта позволяет наделить системы защиты свойством самообучения и обеспечивает обнаружение различного вида "киберугроз". Таким образом, повышается класс защиты объектов.

Литература

1. *Ростовцев В. С.* Искусственные нейронные сети: учебник. — Киров: Изд-во ВятГУ, 2014. — 208 с.

2. *Солдатова О. П.* Нейроинформатика: учебное пособие. — Самара: СГАУ им. С. П. Королева, 2013. — 130 с.

Use of neural networks to provide information protection at sensitive facilities of organizations and institutions

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

The article considers the possibility of using personality identification and information protection systems implemented using neural networks and artificial intelligence elements.

Keywords: information security, neural networks, perceptron, artificial intelligence.

Bibliography — 2 references. *Received February 9, 2021*

ВСЕМ ПУБЛИКАЦИЯМ ВСЕХ НАШИХ НАУЧНЫХ ИЗДАНИЙ БУДЕТ ПРИСВАИВАТЬСЯ КОД DOI!

Издательство ФГУП «НТЦ оборонного комплекса «Компас» заключило с Научной электронной библиотекой договор на оказание услуг по обслуживанию кодов DOI всех научных изданий, начиная с первых выпусков 2021 г.

DOI (Digital Object Identifier) – это уникальный код публикации, указывающий на ее электронное местонахождение, используемый в качестве международного стандарта предоставления информации в сети Интернет. DOI разработан компанией International DOI Foundation (IDF), основанной на членстве регистрационных агентств, предоставляющих конечным пользователям услуги по присвоению префиксов DOI.

Регистрационные агентства назначаются IDF и предоставляют услуги владельцам префиксов DOI: они распределяют префиксы DOI, регистрируют DOI для объектов и предоставляют необходимую инфраструктуру, позволяющую владельцам объектов присваивать DOI и передавать метаданные объектов. CrossRef — это международное регистрирующее агентство, предоставляющее DOI для научных публикаций (книги, журнальные статьи, материалы конференций и т. д.). Научная электронная библиотека с декабря 2019 года является официальным представителем компании CrossRef.

Разработанный компанией Научная электронная библиотека Сервис DOI позволяет без непосредственного участия представителей издательств осуществлять передачу метаданных публикаций в базу данных Crossref. eLIBRARY.RU берет на себя все функции, связанные с проверкой данных, формированием XML-файлов для загрузки в CrossRef, контролем и исправлением возможных ошибок в процессе загрузки. Подавляющее большинство российских научных издательств на регулярной основе размещает информацию в РИНЦ. Эта информация проходит проверку, нормализуется, структурируется и преобразуется в формат, поддерживаемый системой CrossRef. По мере поступления новых публикаций в РИНЦ они автоматически отправляются в CrossRef на регистрацию. Таким образом, подключение к сервису DOI на eLIBRARY.RU избавляет издательства от дополнительных хлопот, связанных с поддержкой DOI в своих изданиях.

В результате оказания услуги **статьям выпусков издательства ФГУП «НТЦ оборонного комплекса «Компас» будет присваиваться уникальный идентификационный номер (DOI), начиная с первых выпусков 2021 года**, с помощью которого можно определить метаданные опубликованных научных статей, их местонахождение в сети Интернет (URL), и иные данные путем обращения к поисковой системе Международного фонда DOI.

Приглашаем к публикации результатов научных разработок и исследований всех тружеников науки: руководителей научных организаций, ведущих научных сотрудников, разработчиков, аспирантов, докторантов в наших научных изданиях!

По материалам сайта: https://www.elibrary.ru

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

ИЗДАТЕЛЬСТВО ФГУП «НТЦ ОБОРОННОГО КОМПЛЕКСА «КОМПАС» ПРЕДЛАГАЕТ:

- ✓ *использовать издания предприятия в качестве информационной площадки Вашей организации;*
- ✓ *осуществлять на регулярной основе публикации в данных журналах научных статей;*
- ✓ *публиковать на страницах изданий*
  - *рекламные и имиджевые материалы Вашей организации;*
  - *обзорные статьи руководителей о последних научно-технических разработках, достижениях, результатах научно-исследовательских работ, проблемах и путях их решений;*
  - *материалы проводимых Вами научно-технических конференций, семинаров и иных отраслевых мероприятий;*
  - *а также любую другую актуальную для Вашей организации информацию, соответствующую тематической направленности журналов.*

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

Издается с 1984 года
ISSN 1729-6552

«Оборонный комплекс — научно-техническому прогрессу России»
научно-технический журнал

Научные специальности журнала:

05.02.02	—	Машиноведение, системы приводов и детали машин;
05.02.05	—	Роботы, мехатроника и робототехнические системы;
05.02.07	—	Технология и оборудование механической и физико-технической обработки;
05.02.13	—	Машины, агрегаты и процессы;
05.02.22	—	Организация производства (по отраслям);
05.12.04	—	Радиотехника, в том числе системы и устройства телевидения;
05.12.07	—	Антенны, СВЧ устройства и их технологии;
05.12.13	—	Системы, сети и устройства телекоммуникаций;
05.12.14	—	Радиолокация и радионавигация;
05.13.06	—	Автоматизация и управление технологическими процессами и производствами (по отраслям);
05.13.10	—	Управление в социальных и экономических системах;
05.13.15	—	Вычислительные машины, комплексы и компьютерные сети;
05.13.18	—	Математическое моделирование, численные методы и комплексы программ.

Издается с 1974 года
ISSN 2073-2600

«Вопросы защиты информации»
научно-практический журнал

Научные специальности журнала:

05.13.01	—	Системный анализ, управление и обработка информации (по отраслям);
05.13.11	—	Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей;
05.13.15	—	Вычислительные машины, комплексы и компьютерные сети;
05.13.18	—	Математическое моделирование, численные методы и комплексы программ;
05.13.19	—	Методы и системы защиты информации, информационная безопасность.

Издается с 1993 года
ISSN 2073-2589

«Экология промышленного производства»
межотраслевой научно-практический журнал

Научные специальности журнала:

05.23.03 — Теплоснабжение, вентиляция, кондиционирование воздуха, газоснабжение и освещение;
05.23.04 — Водоснабжение, канализация, строительные системы охраны водных ресурсов;
05.23.19 — Экологическая безопасность строительства и городского хозяйства;
05.26.06 — Химическая, биологическая и бактериологическая безопасность.

Издается с 1981 года
ISSN 2073-2562

«Конструкции из композиционных материалов»
межотраслевой научно-технический журнал

Научные специальности журнала:

05.07.02 — Проектирование, конструкция и производство летательных аппаратов;
05.07.03 — Прочность и тепловые режимы летательных аппаратов;
05.07.05 — Тепловые электроракетные двигатели и энергоустановки летательных аппаратов;
05.07.07 — Контроль и испытание летательных аппаратов и их систем;
05.16.06 — Порошковая металлургия и композиционные материалы;
05.17.06 — Технология и переработка полимеров и композитов;
05.17.11 — Технология силикатных и тугоплавких неметаллических материалов.

Издается с 1976 года
ISSN 2073-2597

«Информационные технологии в проектировании и производстве»

Научные специальности журнала:

05.11.01 — Приборы и методы измерения (по видам измерений);
05.11.07 — Оптические и оптико-электронные приборы и комплексы;
05.11.08 — Радиоизмерительные приборы;
05.11.14 — Технология приборостроения;
05.11.16 — Информационно-измерительные и управляющие системы (по отраслям);
05.13.05 — Элементы и устройства вычислительной техники и систем управления;
05.13.06 — Автоматизация и управление технологическими процессами и производствами (по отраслям);
05.13.10 — Управление в социальных и экономических системах;
05.13.12 — Системы автоматизации проектирования (по отраслям);
05.13.15 — Вычислительные машины, комплексы и компьютерные сети;
05.13.18 — Математическое моделирование, численные методы и комплексы программ.

Журналы включены решением ВАК Министерства науки и высшего образования Российской Федерации в перечень ведущих рецензируемых научных журналов и изданий. Метаданные выпусков журнала включены в базу данных Российского индекса научного цитирования (РИНЦ).

Отдел научных и информационных изданий
Тел.: 8 (495) 491-43-17, 8 (495) 491-77-20. *Факс:* 8 (495) 491-44-80.
E-mail: secretariat@ntckompas.ru, izdanie@ntckompas.ru, ivleva@ntckompas.ru

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).

БЛАНК-ЗАКАЗ НА ПОДПИСКУ 2021 г.
на издания ФГУП «НТЦ оборонного комплекса «Компас»

Наименование издания	Периодич-ность в год	Цена 1 экз., руб.	Кол-во выпусков в год	Общая сумма, руб.
Оборонный комплекс — научно-техническому прогрессу России	4	1550,00		
Конструкции из композиционных материалов	4	1700,00		
Экология промышленного производства	4	1500,00		
Информационные технологии в проектировании и производстве	4	1750,00		
Вопросы защиты информации	4	1750,00		
В цену включены: НДС — 10 % и стоимость почтовой доставки.				

Поставка журналов подписчикам через издательство осуществляется почтовыми бандеролями с приложением всех необходимых бухгалтерских документов.

Наши реквизиты:

Полное наименование организации: _____

Сокращенное наименование организации: _____

ИНН/КПП _____

ОКПО _____

Расчётный счёт № _____ в _____

к/с _____ БИК _____

Юридический адрес: _____

Почтовый адрес: _____

Контактное лицо _____ тел. _____

E-mail: _____

(Для оформления счёта и бухгалтерских документов просьба заполнить все строчки).

Справочно:
Заполненный бланк-заказ просьба отправить по факсу: 8(495) 491-44-80 или
E-mail: secretariat@ntckompas.ru
Более подробную информацию об изданиях и подписке можно получить по телефону:
8 (495) 491-43-17, 8 (495) 491-77-20.
E-mail: ivleva@ntckompas.ru
Адрес редакции: 125424, Москва, Волоколамское шоссе, д.77.
ФГУП «НТЦ оборонного комплекса «Компас».