ISSN 2073-2600

# ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

3

(134)

*Подписывайтесь,*
*читайте,*
*пишите в наш журнал*

Москва 2021

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

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


Межотраслевой научно-технический журнал

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

Подписной индекс **79379**

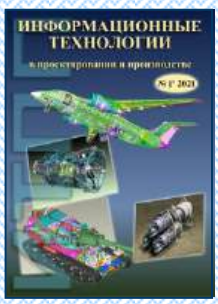
Издается с 1984 года


Межотраслевой научно-технический журнал

**Конструкции из композиционных материалов**
(4 выпуска)

Подписной индекс **80089**

Издается с 1981 года




Научно-технический журнал

**Информационные технологии в проектировании и производстве**
(4 выпуска)

Подписной индекс **79378**

Издается с 1976 года


Межотраслевой научно-практический журнал

**Экология промышленного производства**
(4 выпуска)

Подписной индекс **80090**

Издается с 1993 года


Научно-практический журнал

**Вопросы защиты информации**
(4 выпуска)

Подписной индекс **79187**

Издается с 1974 года

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

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

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

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

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

# ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

**НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ**

**3 (134)**

**Москва 2021**
**Основан в 1974 г.**

## СОДЕРЖАНИЕ



**Главный редактор** ***В. Г. Матюхин,***
д-р техн. наук, первый заместитель генерального директора, научный руководитель ОАО "НИИАС"

**Заместитель главного редактора** ***В. А. Конявский,***
д-р техн. наук, акад. РАЕН, зав. кафедрой МФТИ

**Ответственный секретарь** ***К. В. Трыкина*****,**
начальник отдела научных и информационных изданий ФГУП «НТЦ оборонного комплекса «Компас»

**Редакционная коллегия:**

***М. М. Грунтович,*** канд. физ.-мат. наук, доц., руководитель обособленного подразделения ОКБ САПР; ***С. В. Дворянкин,*** д-р техн. наук, проф., акад. РАЕН, профессор кафедры Финансового университета; ***С. М. Климов*** д-р техн. наук, проф., начальник управления 4 ЦНИИ МО; ***В. П. Лось,*** д-р воен. наук, проф., зав. кафедрой МТУ; ***И. Г. Назаров,*** канд. техн. наук, генеральный директор ОКБ САПР; ***С. П. Панасенко,*** канд. техн. наук, зам. генерального директора по науке и системной интеграции ООО Фирмы "АНКАД"; ***Г. В. Росс,*** д-р техн. наук, д-р эконом. наук, проф., профессор кафедры МТУ; ***В. Ю. Скиба,*** д-р техн. наук, первый зам. начальника Главного управления информационных технологий ФТС России; ***А. А. Стрельцов,*** д-р техн. наук, д-р юр. наук, проф., зам. директора Института проблем информационной безопасности МГУ им. М. В. Ломоносова; ***А. Ю. Стусенко***, канд. юр. наук, зам. директора по безопасности, ФГУП «НТЦ оборонного комплекса «Компас»; ***А. М. Сычёв,*** канд. техн. наук, доц., зам. начальника Главного управления безопасности и защиты информации ЦБ РФ; ***Ю. С. Харин,*** д-р физ.-мат. наук, чл.-кор. НАН Белоруси, директор НИИ прикладных проблем математики и информатики БГУ; ***И. Б. Шубинский,*** д-р техн. наук, проф., генеральный директор ЗАО "ИБТранс", советник генерального директора ОАО "НИИАС"; ***Ю. К. Язов,*** д-р техн. наук, проф., главный научный сотрудник управления ГНИИИ ПТЗИ ФСТЭК России.

© Федеральное государственное унитарное предприятие «НТЦ оборонного комплекса «Компас», 2021

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2021.
Вып. 3 (134). С. 1—60.

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

Подписано в печать 15.09.2021. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 7,0. Уч.-изд. л. 7,2.
Тираж 400 экз. Заказ 1980. 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 004.056
DOI: 10.52190/2073-2600_2021_3_3

# Интеграция СЗИ со службой каталогов Astra Linux Directory: проблемы и подходы

*А. О. Лобач*
Московский физико-технический институт (национальный исследовательский университет), г. Долгопрудный, Московская обл., Россия

*Сформулирована обобщенная схема идентификации/аутентификации (И/А) средств защиты информации (СЗИ). Проведен обзор каталога Astra Linux Directory (ALD). С учетом проведенного анализа предложены и рассмотрены подходы к решению задачи интеграции СЗИ и ALD. В каждом из подходов выделены этапы И/А СЗИ, которые переходят на сторону ALD при их интеграции. Сформулированы общие алгоритмы реализации данных подходов. Выявлены основные проблемы и угрозы выбранных подходов.*

*Ключевые слова:* система защиты информации, Astra Linux Directory, аутентификация, идентификация, угрозы.

При интеграции СЗИ с экосистемой (совокупность сервисов, устройств, прочих продуктов, поддерживаемых одной или разными компаниями и неразрывно связанных в единую сеть определенными организационными и/или технологическими процессами [1]) особое внимание необходимо уделить реализации основных функций защиты от несанкционированного доступа. Прежде всего это идентификация и аутентификация, функции, позволяющие зафиксировать круг лиц, имеющих доступ к объекту, который защищает СЗИ, а также функция разграничения доступа, которая непосредственно определяет права пользователей, прошедших И/А [2].

В свою очередь политика безопасности и правила разграничения доступа формируются на более высоком уровне абстракции по сравнению с уровнем, на котором выполняют базовые функции СЗИ [3]. Современные экосистемы стремятся проводить настройку прав и атрибутов доступа в одном месте с настройкой параметров И/А [4], поэтому возникает необходимость встраивания СЗИ в существующие экосистемы. При таком встраивании часть базовых функций СЗИ будет выполняться в отдельных компонентах данной экосистемы, что может создать дополнительные угрозы, которые не рассматривали при разработке СЗИ. В результате необходимо разобрать, какие способы встраивания СЗИ в экосистему существуют и к проявлению каких угроз они могут привести. Важными условиям этого встраивания являются сохранение высокого уровня безопасности существующих СЗИ и реализация компенсационных мер для вновь появившихся угроз.

В данной статье в качестве примера СЗИ рассматриваются системы линейки Аккорд, которые являются одними из лидирующих продуктов на российском рынке.

В качестве примера экосистемы рассматривается комплекс программ ALD. Стоит отметить, что на текущий момент анонсирован выход новой версии — ALD Pro. Про данную систему нет подробной информации в широком доступе, но по описанию функциональности, которое приводят разработчики в [5], можно сделать вывод, что выделенные подходы интеграции СЗИ с ALD также будут применимы к новой версии ALD Pro.

Программное обеспечение, реализующее функционал единого пространства пользователей (ЕПП), является уязвимым [6, 7] по отношению к внешним угрозам, поскольку механизмы реализации базируются на публичном протоколе и сам сервис является общедоступным, в том числе для злоумышленников. По этой причине целесообразна реализация механизма повышения защищенности сервиса ЕПП в части И/А.

Прежде чем приступить к рассмотрению определенных подходов интеграции СЗИ и ALD, про-

**Лобач Андрей Олегович**, студент.
E-mail: andrey.lobach@mail.ru

*Статья поступила в редакцию 3 августа 2021 г.*

© Лобач А. О., 2021

ведем краткий обзор службы каталогов ALD и представим общую схему И/А СЗИ линейки Аккорд.

### Служба каталогов ALD

Комплекс программ ALD предназначен для организации ЕПП для автоматизированных систем, работающих под управлением ОС Astra Linux.

ALD использует протокол прикладного уровня LDAP (Lightweight Directory Access Protocol), сетевой протокол аутентификации Kerberos 5, сетевую файловую систему CIFS (Common Internet File System) и решает следующие задачи [8]:

- централизованное хранение и управление учетными записями пользователей и групп;
- сквозную аутентификацию пользователей в домене с использованием протокола Kerberos 5;
- функционирование глобального хранилища домашних директорий, доступных по Samba/CIFS;
- автоматическую настройку всех необходимых файлов конфигурации UNIX, LDAP, Kerberos;
- поддержку соответствия БД LDAP и Kerberos;
- создание резервных копий БД LDAP и Kerberos с возможностью восстановления;
- интеграцию в домен входящих в дистрибутив ОС Astra Linux СУБД, серверов электронной почты, веб-серверов, серверов печати и т. п.

### Обобщенная схема И/А в СЗИ

Для формирования возможных подходов механизма интеграции СЗИ в ALD необходимо выделить общую схему И/А в СЗИ.

Исходя из анализа механизмов конкретных видов реализации И/А можно выделить следующие этапы [2], [9, 10]:

1) ввод данных АИП (аутентифицирующая информация пользователя) и учетной информации пользователя;
2) передача в обработку;
3) преобразование данных. Получение данных для сравнения с эталоном (идентификаторы, хэши паролей);
4) получение эталонов из базы;
5) хранение эталонов;
6) сравнение с эталоном плюс дополнительные проверки;
7) принятие решения об успешности И/А;
8) хранение прав пользователя;
9) получение прав пользователя;
10) принятие решения о доступе и правах;
11) предоставление доступа.

При этом регистрация нового пользователя в СЗИ осуществляется следующим образом:

- администратор присваивает пользователю уникальное имя в системе;
- происходит настройка параметров учетной записи пользователя:
  - персональный идентификатор;
  - пароль;
  - данные аутентификации.

Дополнительно можно выполнить настройку следующих параметров [8, с. 17]:

- параметры пароля;
- атрибуты доступа;
- результаты И/А.

### Предлагаемые подходы по интеграции СЗИ с ALD

С учетом обобщенной схемы И/А СЗИ и функционала ALD выделим следующие подходы.

***Использование ALD как инструмента идентификации/аутентификации.*** Идея использования службы каталогов как способа аутентификации возникла из анализа источника [11]. В [11] в качестве службы каталогов выступает AD. Поскольку в основе AD и ALD лежат реализации протокола LDAP, выбор данного подхода применительно к ALD представляется перспективным.

При использовании данного подхода необходимо дублировать хранилище пользователей в СЗИ и ALD, поскольку при прохождении И/А ALD необходимо подтверждать введенный пароль пользователя, т. е. данные о пользователях обязательно должны сохраняться и в ALD. Соответственно этапы 2—7 (непосредственно аутентификация) обобщенной схемы И/А в СЗИ дублируются в ALD. Авторизация пользователя происходит исключительно на стороне СЗИ (этапы 8—11).

Регистрация нового пользователя происходит и в СЗИ, и в ALD. При этом в ALD сохраняется только та информация, которая требуется для аутентификации (идентификаторы, хэши паролей).

Реализация предполагает создание информационной системы, которая позволит осуществлять ведение информации о пользователях в СЗИ и проведение И/А на стороне ALD, одновременно с этим при регистрации новых пользователей в ALD позволит обновлять матрицу доступа в СЗИ.

Предлагаемый алгоритм работы информационной системы следующий:

- получаем идентификатор пользователя;
- посредством Kerberos подтверждаем существование такого пользователя в ALD;

- если пользователь зарегистрирован в ALD, СЗИ запрашивает пароль, в противном случае выдается сообщение об ошибке и процесс аутентификации прерывается;
- введенный пароль используется для аутентификации пользователя посредством СЗИ.

Недостатком данного подхода является необходимость обеспечения синхронизации данных пользователей между базами данных СЗИ и ALD, а также дублирование хранилища пользователей, что может отрицательно повлиять на уровень защищенности всей системы.

Кроме того, происходит некоторое снижение быстродействия из-за необходимости взаимодействия распределенных систем, а также возникает задача администрирования/поддержки работы инфраструктуры (на узлах должна быть обеспечена установка единого времени) [12].

***Хранение базы данных СЗИ в облаке, т. е. полное перенесение данных в ALD.*** Возможность работы с атрибутами пользователя ALD подтверждается наличием доступных библиотек для доступа к публичным интерфейсам OpenLDAP в составе ALD [13]. Появляется возможность хранения вне контура СЗИ данных пользователя, которые необходимы для выполнения процедуры И/А.

При таком подходе данные пользователя хранятся в ALD. При предъявлении пользователем идентификатора СЗИ обращается к ALD. В случае введения существующего идентификатора ALD передает в СЗИ данные о пользователе (например, хэш-пароль) для последующей аутентификации. Если пользователь вводит верный пароль, аутентификация считается пройденной.

При использовании данного подхода СЗИ делегирует ALD этапы 4, 5 обобщенной схемы И/А СЗИ (хранение и получение эталонов), а также этапы 8, 9 (хранение и получение прав пользователей).

Соответственно регистрация нового пользователя осуществляется в СЗИ, но при этом результаты регистрации сохраняются в ALD.

Реализация предполагает создание информационной системы, которая позволит хранить и получать данные о пользователях из ALD и при этом выполнять операции И/А на стороне СЗИ.

Предлагаемый алгоритм работы системы следующий:

- получение идентификатора пользователя;
- выполнение запроса в базу данных ALD в целях получения атрибутов пользователя, необходимых для проведения процедуры аутентификации (например, хэш-пароля);
- в случае, если данный пользователь обнаружен в базе данных ALD, проведение аутентификации пользователя посредством СЗИ;
- если введенный пароль совпал, процесс аутентификации успешно завершается.

В данном подходе все данные хранятся в ALD, соответственно, увеличивается вероятность их компрометации.

При этом не задействуются механизмы И/А ALD, поэтому данный подход является менее защищенным, чем альтернативные.

***Данные о пользователях остаются локальными и синхронизируются с данными в ALD.*** В соответствии с аргументами, описанными ранее, наличие публичных интерфейсов OpenLDAP [13] позволяет осуществлять синхронизацию данных пользователей в ALD и СЗИ.

Актуальные данные пользователя хранятся в ALD. Периодически эти данные копируют в локальное хранилище СЗИ. При предъявлении пользователем идентификатора СЗИ обращается к локальной базе. В случае, если в локальной базе данные не обнаружены, выполняется запрос в ALD для их обновления по конкретному идентификатору. Если требуемый идентификатор пользователя существует, СЗИ выполняет запрос пароля. После этого происходит аутентификация пользователя по данным из хранилища.

Таким образом, в данном подходе в ALD дублируются 4-й и 5-й этапы обобщенной схемы И/А СЗИ (хранение и получение эталонов), а также 8-й и 9-й этапы (хранение и получение прав пользователей).

Регистрация нового пользователя осуществляется на стороне СЗИ, после чего результат регистрации сохраняется в ALD. При входе этого пользователя локальная база СЗИ будет обновлена путем обмена данными с ALD.

Для реализации указанного подхода необходимо создание системы, которая выполняет периодическую или по событию (в случае ошибок, связанных с данными из локальной базы) синхронизацию данных по пользователям из ALD в локальную базу.

Предлагаемый алгоритм работы системы следующий:

- получение идентификатора пользователя;
- выполнение запроса в локальную базу данных СЗИ для осуществления идентификации;
- в случае, если в локальной базе идентификатор пользователя не обнаружен, выполнение запроса в базу данных ALD. При этом в локальную базу данных СЗИ происходит копирование актуальной информации по пользователю;

- в случае успеха (идентификатор существует) осуществляется запрос пароля пользователя и начинается выполнение процедуры аутентификации;
- в случае ошибки аутентификации снова происходят обращение к базе данных ALD и обновление информации в локальной базе по конкретному пользователю для обработки случаев, когда пароль пользователя был изменен в ALD, но синхронизация с локальным хранилищем еще не выполнена;
- если введенный пароль совпал, процесс аутентификации успешно завершается.

При данном подходе синхронизация осуществляется за счет периодического опроса данных пользователей в ALD, и в случае, если интервал опроса недостаточно короткий, синхронность данных в СЗИ и ALD может быть нарушена.

Показательным примером такого нарушения является то, что реализация допускает возможность успешной аутентификации пользователя, который был удален в ALD.

Данный подход является лучшим с точки зрения быстродействия, но более сложным в реализации, чем альтернативные варианты.

## Заключение

Каждый из приведенных подходов имеет свои преимущества и недостатки. При этом можно выделить ряд угроз, касающихся всех походов: угрозы, связанные с доверием к маршруту и каналу СЗИ—ALD, а также угрозы, связанные с корректной работой управления атрибутами безопасности (идентификаторы, группы, роли и т. д.) [11]. Также можно выделить общую проблему, которая заключается в том, что все эталоны хранятся в ALD, что является уязвимым местом приведенных подходов. Однако для первого подхода эта уязвимость наименее критична, поскольку атрибуты доступа хранятся только в СЗИ.

Первый подход, использующий возможности ALD для И/А, является самым защищенным, но неэффективным с точки зрения быстродействия, поскольку все обращения приводят к запросам в ALD.

Второй подход является также относительно медленным по тем же причинам, что и в первом случае. При этом он недостаточно защищен по сравнению с первым подходом.

Третий подход — самый быстродействующий по сравнению с альтернативными подходами, поскольку в нём минимизированы обращения к внешнему сервису (ALD) в процессе аутентификации. Однако данный подход допускает возможность ложной аутентификации.

По указанным причинам для реализации стоит выбирать между первым и третьим подходами в зависимости от того, что находится в приоритете: повышенная защищенность системы или ее быстродействие.

**Литература**


1. *Сухов Р., Исаев Е., Мальцева С.* Доклад "Экосистемы в информационных технологиях". — М., 2017. — 12 с.
2. *Щеглов А., Щеглов К.* Идентификация и аутентификация. Так ли все просто? [Электронный ресурс]. URL: https://ecm-journal.ru/post/Identifikacija-i-autentifikacija-Tak-li-vse-prosto.aspx (дата обращения: 22.05.2021).
3. *Богаченко Н. Ф.* Анализ проблем управления разграничением доступа в крупномасштабных информационных системах // Математические структуры и моделирование. 2018. № 2(46). С. 135—152.
4. Единая система идентификации и аутентификации в инфраструктуре электронного правительства РФ (ЕСИА) // Zdrav. Expert. 2020 [Электронный ресурс]. URL: https://zdrav.expert/index.php/Статья:Единая_система_идентификации_и_аутентификации_в_инфраструктуре_электронного_правительства_РФ_(ЕСИА) (дата обращения: 26.07.2021).
5. Презентация ALD Pro. [Электронный ресурс]. URL: https://astralinux.ru/information/materials/prezentacziya-ald-pro-resheniya-dlya-avtomatizaczii-czentralizovannogo-upravleniya.pdf (дата обращения: 26.07.2021).
6. *Ализар А.* Обход аутентификации в pam_ldap. 11 марта 2006 [Электронный ресурс]. URL: https://xakep.ru/2006/11/03/34885/ (дата обращения: 29.05.2021).
7. *Ализар А.* Обход ограничений безопасности в OpenLDAP. 9 июня 2006 г. [Электронный ресурс]. URL: https://xakep.ru/2006/09/06/33701/ (дата обращения: 29.05.2021).
8. Справочный центр Astra Linux [Электронный ресурс]. URL: https://wiki.astralinux.ru/display/doc/Astra+Linux+Directory (дата обращения: 29.05.2021).
9. ПАК СЗИ от НСД для ПЭВМ (РС) "Аккорд-АМДЗ". Руководство администратора. М.: ОКБ САПР, 2019. — 121 с. [Электронный ресурс]. URL: https://www.okbsapr.ru/upload/iblock/f86/f86fb0fdbaa07b51afa3cafc2c96eeda.pdf
10. ПАК СЗИ от НСД "Аккорд-Win64" (версия 5.0). Руководство администратора. М.: ОКБ САПР. — 101 с. [Электронный ресурс]. URL: https://www.okbsapr.ru/upload/iblock/e86/e86f0a022bb079b46f4e3a10375054d8.pdf
11. *Похачевский Д. А.* О некоторых угрозах СДЗ, использующих ACTIVE DIRECTORY для решения задач аутентификации и авторизации: мат. XXIV Научно-практ. конф. "Комплексная защита информации" Витебск. 21—23 мая 2019 г.: УО ВГТУ. — Витебск, 2019. С. 376—380.
12. *Шнайер Б.* Глава 3. Основные протоколы. Протокол Kerberos // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. С. 81.
13. *Yves Legrandgerard* libldap Documentation. Release 0.1. 2017 г. [Электронный ресурс]. URL: https://readthedocs.org/projects/libldap/downloads/pdf/stable/ (дата обращения: 29.05.2021).

# Integration of Information Security System with the Astra Linux Directory service: problems and approaches

*A. O. Lobach*
Moscow Institute of Physics and Technology (National Research University), Dolgoprudny, Moscow region, Russia

*In this article, a generalized scheme of identification/authentication (hereinafter referred to as I/A) of the Information Security System (ISS) is formulated. The Astra Linux Directory (ALD) is reviewed. Based on this, approaches to solving the problem of integration the ISS and ALD are proposed and considered. In each of the approaches, the stages I/A of ISS that pass to the ALD side during their integration are highlighted. General algorithms for the implementation of these approaches are formulated. The main problems and threats of the selected approaches are also identified.*

*Keywords:* information security system, Astra Linux Directory, authentication, identification, threats.

Bibliography — 13 references. *Received August 3, 2021*

УДК 004.056
DOI: 10.52190/2073-2600_2021_3_8

# Применение TLA+ нотации для описания модели изолированной программной среды субъектов доступа и ее дальнейшей верификации

*А. М. Каннер*
ЗАО "ОКБ САПР", Москва, Россия

*Рассматриваются недостатки верификации математических нотаций моделей безопасности. Предлагается использование темпоральной логики действий Лэмпорта для представления моделей безопасности на формальном языке, пригодном для верификации с применением инструментальных средств. Рассматривается модель изолированной программной среды субъектов доступа, приводится ее спецификация в TLA+ нотации, описываются достоинства верификации данной спецификации с использованием инструментальных средств.*

*Ключевые слова:* модель ИПСС, спецификация модели ИПСС, верификация модели ИПСС, темпоральная логика действий Лэмпорта, TLA+, метод Model Checking.

Все более актуальной становится необходимость проведения моделирования и верификации разрабатываемых средств защиты информации (СЗИ). Это связано в том числе с требованиями, предъявляемыми в ряде нормативных документов Российской Федерации к верификации функций защиты СЗИ [1, 2]. Для верификации средств защиты информации используют специальные инструментальные средства, которые позволяют проверить выполнение некоторых формальных свойств при работе данных СЗИ в автоматическом режиме. При этом такие инструментальные средства позволяют проверять в автоматическом режиме не только средства защиты информации, но и математические модели безопасности компьютерных систем.

Существующие наиболее известные формальные модели безопасности, например Белла—ЛаПадулы, сформулированы в математической нотации, с использованием некоторого математического аппарата. При этом основным компонентом таких формальных моделей является базовая теорема безопасности, с помощью которой обосновывают формальные свойства, гарантирующие безопасность системы или обрабатываемых в ней данных. Для модели Белла—ЛаПадула формальным свойством, гарантирующим безопасность данных, является невозможность возникновения информационных потоков "сверху вниз" — утечки информации с большего уровня конфиденциальности на меньший.

Необходимо отметить, что любая формальная модель в математической нотации имеет достаточно сложное описание, ошибки в базовой теореме безопасности или в самой нотации может выявить только квалифицированный специалист-математик, поэтому при проверке математической нотации всегда необходимо учитывать человеческий фактор. Однако даже после верификации модели в ней могут существовать скрытые пропущенные недостатки. При этом проверка моделей безопасности на наличие ошибок является важной задачей, так как такие модели используют в качестве фундамента для теоретической гарантии некоторых свойств безопасности в компьютерных системах.

В связи с этим для проверки формальных моделей безопасности предложено использовать инструментальные средства автоматической верификации, а математическую нотацию перевести в нотацию на некотором формальном языке, пригодном для верификации, например TLA+ (Temporal Logic of Actions). На основании данной нотации можно сформулировать условия базовой теоремы безопасности в виде инвариантов или темпоральных свойств.

Использование инструментальных средств автоматической верификации позволяет исключить человеческий фактор при проверке модели безопасности и проводить верификацию силами менее квалифицированных специалистов, осуществляющих только запуск средств верификации. Помимо этого такая верификация позволяет проверять выполнение условий базовой теоремы без-

**Каннер Андрей Михайлович**, программист группы программирования ПО для СЗИ отдела программирования СЗИ.
E-mail: kanner@okbsapr.ru

*Статья поступила в редакцию 1 июля 2021 г.*

© Каннер А. М., 2021

опасности во всевозможных состояниях моделируемой системы и выявлять скрытые ошибки в математической нотации.

## Материалы и методы

В работе автора [3] приведено описание математической нотации модели изолированной программной среды субъектов доступа (ИПСС), которая является развитием субъектно-ориентированной модели изолированной программной среды (ИПС) [4, 5]. В модели ИПСС в отличие от ИПС предлагается другое представление сущностей системы:

- субъекты — это пользователи и системные сервисы, а не процессы пользователей, как в ИПС;
- объекты — функционально ассоциированные с субъектами объекты (процессы) и объекты-данные с возможностью динамического изменения их состава во времени.

При этом модель ИПСС имеет следующие основные отличия от модели ИПС:

- осуществляется учет подсистемы защиты в качестве сущности системы, такой же, как и другие субъекты системы;
- приводится обоснование невозможности нарушения действующих правил управления доступом за счет свойства абсолютной корректности (изолированности) субъектов доступа.

Как уже было сказано, математическая нотация модели не позволяет гарантировать выполнения формальных свойств безопасности во всех возможных состояниях системы, а экспериментальные исследования реализаций этой модели на практике требуют повторного проведения даже при малых усовершенствованиях модели. В связи с этим авторами работы [6] проведена верификация модели ИПСС с использованием темпоральной логики действий Лэмпорта и метода Model Checking.

Спецификация модели ИПСС в TLA+ имеет следующие компоненты:

- начальное состояние — инициализация системы (Init), предикат инициализации модели ИПСС;
- переменные модели — сущности, которые могут изменяться в процессе работы (субъекты, объекты и т. д.);
- правила работы системы — возможные состояния и значения переменных модели, правила перехода из состояния в состояние, например при осуществлении доступов субъектов к объектам;
- теорема, доказываемая при верификации и проверяющая специальные предикаты (формальные свойства системы) — инварианты и темпоральные свойства.

В качестве действий в системе могут совершаться запросы модели ИПСС: создание и удаление процессов, создание пользователей и системных субъектов, удаление субъектов, а также чтение, запись, создание, удаление и исполнение объектов доступа. Предусловиями являются предикаты, выполнение которых необходимо для совершения действия. Постусловия определяют, каким образом после выполнения действия изменяются переменные модели, т. е. какое новое состояние будет иметь система.

При доказательстве теоремы в ходе верификации проверяется истинность специальных предикатов — следующих инвариантов или темпоральных свойств:

Invariants and Temporal Properties

Теорема, учитывающая инварианты и свойства: доказывается при верификации

THEOREM $Spec \Rightarrow \wedge \Box\, TypeInv$
$\wedge \Box\, ConsistencyInv$
$\wedge \Box\, BlockedInv$
$\wedge \Box\, OSKernelExists$
$\wedge \Box\, SormInits$
$\wedge \Box\, Correctness$
$\wedge \Box\, AbsCorrectnessOpp$
$\wedge\, OSUsabilityLiveness$
$\wedge\, AbsCorrectness$

Инварианты должны выполняться во всех состояниях и для каждой реализации системы. Также инварианты могут проверять условия в прошлом (например, при последнем переходе системы), используя при этом последовательности совершенных запросов к системе. В отличие от инвариантов, темпоральные свойства могут применять специальные темпоральные операторы TLA+ [6, 7]. С помощью этих операторов можно составлять предикаты, зависящие от времени выполнения и определенных событий в прошлом или будущем.

При создании TLA+ нотации модели ИПСС были выявлены скрытые ошибки математической нотации:

- нарушаются инварианты свойств корректности модели ИПСС и один субъект может опосредованно воздействовать на другой субъект доступа через операции порождения;
- существует возможность некорректной работы моделируемой системы, которая проходит этап инициализации, принимает несколько состояний и в одном из таких состояний система пере-

стает работать еще до появления пользователей из-за завершения работы единственного системного процесса — ядра ОС;

- существует возможность работы системы при завершении работы субъекта, разграничивающего доступ, или при удалении объекта, содержащего применяемые правила доступа.

Данные ошибки исправлены в TLA+ нотации. Для этого выполнена модификация свойств корректности и некоторых операций модели ИПСС, а также добавлены следующие инварианты:

*OSKernelExists*
В любой момент времени существует *s_0*
*OSKernelExists* $\triangleq$
$\wedge$ *s_0* $\in$ *S_active*
$\wedge$ *s_0.is_blocked* = FALSE

*SormInits*
В начальный момент времени инициализирован *s_sorm* либо функционирует только *s_0*
SormInits $\triangleq$
$\wedge$ $\vee$ $\wedge$ *s_sorm* $\in$ *S_active*
$\wedge$ *s_sorm.is_blocked* = FALSE
$\vee$ $\wedge$ *s_sorm* $\notin$ *S_active*
$\wedge$ *S_active* = {*s_0*}

OSUsabilityLiveness
Свойство возможности использования ОС
OSUsabilityLiveness $\triangleq$
хотя бы в одном состоянии есть субъекты, кроме
*s_0* и *s_sorm*: пользователь или системный субъект
$\Diamond$ (*Cardinality*(*S_active*) > 2)

где OSKernelExists — инвариант для контроля работоспособности системы (постоянное наличие системного субъекта — ядра ОС);
SormInits — инвариант для контроля активизации подсистемы управления доступом;
OSUsabilityLiveness — темпоральное свойство для проверки работоспособности системы: в любой реализации системы обязательно, кроме начальных системных субъектов, должен активизироваться пользователь или еще один системный субъект.

## Заключение

В результате проведенной верификации формальной модели ИПСС показано, что при верификации моделей безопасности компьютерных систем с использованием классической математической нотации возникает ряд существенных недостатков и целесообразно использовать нотацию именно на пригодных для верификации формальных языках. При этом верификацию следует проводить с использованием специальных инструментальных средств автоматической верификации, а при необходимости транслировать с их помощью описание модели с формального языка в математическую нотацию. Также необходимо отметить, что средства автоматической верификации рекомендуется использовать при написании новых моделей безопасности, так как логические ошибки можно устранять уже на раннем этапе, постепенно добавляя требуемые инварианты безопасности по мере описания основных операций модели.

Полный текст разработанной спецификации модели ИПСС доступен на сайте автора https://github.com/kanner/ipes-model

**Литература**


1. *Каннер А. М.* Подход к верификации подсистемы управления доступом операционной системы Linux: мат. XXV Научно-практ. конф. "Комплексная защита информации" 15—17 сентября 2020 г. — М.: Медиа Группа "Авангард", 2020. С. 24—28.
2. *Каннер А. М., Каннер Т. М.* Моделирование и верификация подсистемы управления доступом средства защиты информации Аккорд-Х // Вопросы защиты информации. 2020. № 3. С. 6—10.
3. *Kanner A. M.* Correctness of Data Security Tools for Protection against Unauthorized Access and their Interaction in GNU/Linux // Global J. Pure and Applied Mathematics. 2016. V. 12. № 3. P. 2479—2501.
4. *Щербаков А. Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009. — 352 с.
5. *Щербаков А. Ю.* Хрестоматия специалиста по современной информационной безопасности. Т. 1. — Saarbrucken: Palmarium Academic Publishing, 2016. — 272 с.
6. *Kanner A. M., Kanner T. M.* Verification of a Model of the Isolated Program Environment of Subjects Using the Lamport's Temporal Logic of Actions: Proceedings of the VII International Conference "Engineering & Telecommunication", IEEE. 2020.
7. *Kanner A. M., Kanner T. M.* Special Features of TLA+ Temporal Logic of Actions for Verifying Access Control Policies: Proceedings of Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, IEEE. 2021 (статья принята к публикации).

# Application of TLA+ notation for describing the model of isolated program environment of subjects and it's further verification

*A. M. Kanner*
JSC "OKB SAPR", Moscow, Russia

*The article considers the disadvantages of verification of mathematical notations of the security models. It is proposed to use the Lamport's temporal logic of actions to represent the security models in a formal language suitable for verification which will be held using specialized tools. The model of isolated program environment of subjects is considered, it's specification is given in TLA+ notation, and the advantages of verifying this specification using specialized tools are described.*

*Keywords:* IPES model, IPES model specification, IPES model verification, Lamport's temporal logic of actions, TLA+, Model Checking method.

Bibliography — 7 references. *Received July 1, 2021*

УДК 004.056
DOI: 10.52190/2073-2600_2021_3_12

# Алгоритм тестирования функций безопасности программно-аппаратных СЗИ, основанный на использовании теории графов

*Т. М. Каннер*
ЗАО "ОКБ САПР", Москва, Россия

*Рассмотрены существующие подходы к тестированию программно-аппаратных средств защиты информации (СЗИ), позволяющие обеспечить полноту тестирования, но не решающие вопрос его оптимальности. Дано определение задачи тестирования программно-аппаратных СЗИ. Предложен подход к проверке ее выполнимости с использованием теории графов. Представлен основанный на данном подходе алгоритм тестирования функций безопасности программно-аппаратных СЗИ, позволяющий обеспечить его полноту и оптимальность.*

*Ключевые слова:* тестирование программно-аппаратных СЗИ, полнота и оптимальность тестирования, ориентированный граф без петель и кратных дуг, алгоритм тестирования функций безопасности программно-аппаратных СЗИ, задача китайского почтальона, эйлеров путь.

При разработке программно-аппаратных средств защиты информации, как и любых других программных или программно-аппаратных средств, должно быть проведено их тестирование в целях подтверждения соответствия реализованных функциональных возможностей заявленным характеристикам.

Существующие подходы к тестированию программных и программно-аппаратных средств предполагают построение математических моделей с применением какого-либо математического аппарата. Во многих случаях (см., например [1—4]) в качестве такого аппарата используют теорию автоматов и поведение СЗИ моделируется при помощи выполнения переходов автомата и получения его выходных значений. В работах [5, 6] автор также выбрал подход к тестированию программно-аппаратных СЗИ, основанный на построении его математической модели. В [5] сформулирована описательная модель, и на ее основе предложена формальная модель произвольного программно-аппаратного СЗИ. В [6] на основании полученной математической модели предложено представление программно-аппаратного СЗИ в виде конечного детерминированного автомата:

$\tilde{m} = (V, I, O, f, g)$ — конечный детерминированный автомат, моделирующий $m \in M$,

где $M$ — множество всех программно-аппаратных СЗИ;

$m$ — произвольное программно-аппаратное СЗИ;

$V$ — множество состояний автомата, $v_0$ — начальное состояние;

$I$ — множество входов (стимулов) — функций $m$, которые могут выполняться в $v \in V$;

$O = \{1, 0\}$ — множество выходов (реакций) — результатов выполнения стимулов в $v \in V$ (успешное или неуспешное выполнение);

$f : I \times V \to V$ — функция переходов: если $f((i, v)) = v'$, то по стимулу $i \in I$ из состояния $v \in V$ автомат переходит в состояние $v' \in V$;

$g : I \times V \to O$ — функция выходов: если $g((i, v)) = o$, то по стимулу $i \in I$ из состояния $v \in V$ на выход автомата поступает $o \in O$.

Предложенный подход, как и другие подходы, основанные на использовании теории автоматов, позволяет обеспечить полноту тестирования программно-аппаратных средств защиты информации. Однако существенным недостатком этих подходов является отсутствие ответа на вопрос об оптимальности выполняемого тестирования. Для обеспечения не только полноты, но и оптимальности в [6] автором введены следующие понятия и сформулирована задача тестирования программно-аппаратного СЗИ:

$V_{ФБ}$ — множество состояний автомата с потенциально вычислимыми ФБ — состояний, в которых необходимо проверить функции безопасности $m$, $V_{ФБ} \subseteq V$;

$T$ — множество всевозможных переходов автомата; при каждом переходе $(v, i, o, v')$ выполняется $f((i, v)) = v'$ и $g((i, v)) = o$, $T \subseteq V \times I \times O \times V$;

**Каннер Татьяна Михайловна**, руководитель учебного центра.
E-mail: tatianash@okbsapr.ru

*Статья поступила в редакцию 1 июля 2021 г.*

© Каннер Т. М., 2021

$\bar{s}$ — последовательность переходов тестирования $s_0, \ldots, s_{l-1} \in T$ длины $\text{len}(\bar{s}) = l \in \mathbb{N}$;

$S$ — множество последовательностей переходов тестирования различной длины.

Для моделируемого автоматом $\tilde{m} = (V, I, O, f, g)$ программно-аппаратного СЗИ $m$ решена задача тестирования с помощью последовательности переходов тестирования $\bar{s} \in S$, когда одновременно выполняются условия:

- возможности проведения тестирования: $m \in M_p$ (где $M_p$ — множество программно-аппаратных СЗИ, для которых вне зависимости от человеческого фактора возможно выполнение ручного тестирования, $M_p \subseteq M$);
- полноты тестирования: $\forall s_j \in T$, для которого $v'_{j+1} \in V_{\text{ФБ}}$ является элементом последовательности $\bar{s}$;
- оптимальности тестирования: $\text{len}(\bar{s}) = \min\{\text{len}(\bar{s}') : \forall \bar{s}' \in S$ выполняется предыдущий пункт$\}$.

В данной работе представлен основанный на предложенном в [6] подходе алгоритм тестирования функций безопасности программно-аппаратных СЗИ, использующий известные алгоритмы теории графов и позволяющий провести тестирование функций безопасности таких СЗИ, а также обеспечить его полноту и оптимальность.

## Алгоритм тестирования функций безопасности программно-аппаратных СЗИ

По аналогии с [6] введем граф:

$G_m = (V, E)$ — ориентированный граф без петель и кратных дуг (простой орграф), соответствующий программно-аппаратному СЗИ, представленному в виде формальной модели в [5], где:

$V$ — множество вершин графа, соответствующих состояниям программной или аппаратной компоненты СЗИ;

$E \subseteq V \times V$ — множество ориентированных ребер (дуг) графа — переходов СЗИ из одного состояния в другое при выполнении нецелевых функций или функций безопасности.

Из условия полноты в задаче тестирования следует, что из некоторой начальной вершины $v_0 \in V$ должен осуществляться обход только тех дуг графа, входящих в вершины, в которых могут выполняться какие-либо функции безопасности СЗИ: $V_{\text{ФБ}} \subseteq V$, а не по всему множеству $V$. Поэтому вместо графа $G_m$ будем рассматривать производный от него граф $G'_m$, который строится с помощью удаления из оригинального графа неиспользуемых при решении задачи тестирования вершин и дуг. Удаление таких вершин и дуг выполняется с использованием приведенных в [6] правил для сохранения связности оставшихся вершин.

При этом обеспечение полноты и оптимальности тестирования основано на поиске пути, проходящего через все дуги хотя бы по одному разу за минимальное количество переходов. Таким образом, в соответствии с [6—9] задача тестирования сводится к задаче китайского почтальона (Chinese postman problem), также известной как задача инспекции дорог (Route Inspection Problem), либо, как частный случай, — к задаче поиска эйлерова пути (Eulerian path / Eulerian trail).

В соответствии с этим на основе [6] можно предложить алгоритм решения задачи тестирования функций безопасности программно-аппаратного СЗИ, который заключается в выполнении следующих шагов.

1. Построить из изначального графа программно-аппаратного СЗИ $G_m$ соответствующий граф $G'_m$ с помощью удаления неиспользуемых при решении задачи тестирования некоторых вершин и дуг, используя приведенные в [6] правила для сохранения связности оставшихся вершин.

2. Если в $G'_m$ есть изолированные вершины (не удаленные при построении графа $G_m$), задача тестирования не может быть решена, так как невозможно выполнить условие полноты тестирования из [6].

3. Проверить, что в $G'_m$ любая вершина $v \in V$ либо принадлежит орцепи, либо лежит в компоненте сильной связности. Это можно сделать с использованием алгоритма Косараджу—Шарира задва обхода графа в глубину [7, 10, 11]: найти все компоненты связности и проверить связанность начальной вершины $v_0$ со всеми остальными вершинами. В противном случае задача тестирования не может быть решена, поскольку также невозможно будет выполнить условие полноты из [6].

4. Для всех вершин графа $G'_m$ необходимо вычислить разницу полустепеней выхода и полустепеней входа. Если в графе есть только сбалансированные вершины (разница равна 0), то в графе существует эйлеров цикл. Если в графе есть только две несбалансированные вершины с разницей 1 и -1, а остальные вершины сбалансированные, то в графе существует эйлеров путь. В этих случаях необходимо продолжить алгоритм с пункта 9.

5. В противном случае требуется рассмотреть отдельно несбалансированные вершины в целях нахождения путей, которые необходимо пройти повторно с сохранением требования по минимизации обхода дуг из условия оптимальности тестирования в [6]. Несбалансированные вершины можно представить в виде биграфа.

6. С помощью алгоритма поиска кратчайших путей для всех вершин в полученном биграфе — алгоритма Флойда—Уоршелла [7, 10] — вычислить длину кратчайших путей от вершин с отрицательной разницей полустепеней выхода и входа к вершинам с положительной разницей.

7. Выбрать с использованием Венгерского алгоритма, алгоритма Куна—Манкреса или алгоритма Форда—Фалкерсона [7, 10] из всех сочетаний возможных кратчайших путей те пути, при повторном использовании которых все вершины станут сбалансированными, но при этом суммарная длина этих путей будет минимальна. При добавлении пути от вершины с отрицательной разницей полустепеней выхода и захода к вершине с положительной разницей разница в обеих вершинах изменится ровно на 1 (для первой — увеличится на 1, для второй — уменьшится на 1). При этом для всех остальных вершин разница не изменится, так как могут добавиться только входящая и исходящая дуга (суммарная разница останется равной 0).

8. Добавить дуги для выбранных на предыдущем шаге дополнительных путей в граф $G'_m$. Так как теперь все вершины сбалансированы, будет существовать эйлеров цикл.

9. С помощью алгоритма на основе циклов, также известного как алгоритм Хиерхольцера [9], построить эйлеров цикл в полученном графе. Посещение достроенных на предыдущем шаге дуг эквивалентно повторному посещению соответствующих дуг графа $G'_m$. Некоторые итерации эйлерова цикла можно менять местами, так как оптимальное решение может быть не единственным.

## Сложность предложенного алгоритма тестирования функций безопасности программно-аппаратных СЗИ

Из предложенного алгоритма решения задачи тестирования программно-аппаратных СЗИ видно, что его шаги выполняются последовательно и для них не используется вложенность. Это означает, что его сложность алгоритма равна максимальной сложности используемых в нем известных алгоритмов на графах. Сложности используемых алгоритмов следующие [6, 7, 9]:

- Сложность построения графа $G'_m$ для представления графа в виде матрицы смежности $O\left(|V'|^3\right)$. За $O\left(|V'|^3\right)$ выполняется первая проверка при построении $G'_m$, за $O\left(|V'|^2\right)$ — вторая и третья, четвертая — за $O\left(|V'|^3\right)$. Соответственно общая сложность не превосходит сложности первой или четвертой проверки.
- Алгоритм Косараджу—Шарира — $O\left(|V'|^2\right)$ для матрицы смежности.
- Расчет полустепеней выхода и входа и их разницы для каждой вершины — $O\left(|V'|^2\right)$ для матрицы смежности.
- Алгоритм Флойда—Уоршелла — $O\left(|V'|^3\right)$.
- Венгерский алгоритм — $O\left(|V'|^3\right)$.
- Алгоритм Хиерхольцера — $O\left(|E'|\right)$.

Таким образом, в случае, если $G'_m$ содержит эйлеров путь (цикл) или не содержит, сложность алгоритма составляет $O\left(|V'|^3\right)$ для представления графа в виде матрицы смежности. То есть задача тестирования программно-аппаратных СЗИ принадлежит классу задач *P*, а не *NP*, и существует алгоритм, решающий эту задачу за полиномиальное время [9].

Предложенный алгоритм подразумевает обход вершин графа с помощью одной последовательности переходов. В случае, если обход графа по приведенному алгоритму невозможно выполнить с помощью одной последовательности переходов, в графе имеется несколько несвязанных ветвей. Следовательно, в СЗИ есть ошибка, так как нельзя добиться, чтобы все функции безопасности выполнялись корректно без нарушения работы других функций безопасности. Поэтому в работе не рассматривается вариант с несколькими последовательными обходами графа СЗИ.

## Апробация предложенного алгоритма тестирования функций безопасности программно-аппаратных СЗИ

Для апробации данного алгоритма были произвольно выбраны два программно-аппаратных СЗИ, относящихся к различным видам [5]:

- ШИПКА, функции безопасности которого реализованы на базе мобильной аппаратной компоненты и взаимодействуют со средой ОС средства вычислительной техники (СВТ);

- СЗИ от несанкционированного доступа "Аккорд-АМДЗ", функции безопасности которого реализованы на базе стационарной аппаратной компоненты и не взаимодействуют с ОС СВТ, выполняются независимо от ОС в составе СВТ.

Для перечисленных средств защиты информации построены соответствующие графы и применен предложенный алгоритм. Показано, что оба графа для данных СЗИ являются сильно связными, т. е. может быть построен оптимальный путь, проходящий по всем ребрам. Это значит, что с использованием предложенного алгоритма может быть получено решение задачи тестирования выбранных СЗИ. При этом будут обеспечены его полнота и оптимальность.

## Заключение

Предложенный алгоритм подразумевает обход вершин графа с помощью одной последовательности переходов, если обход графа по приведенному алгоритму невозможно выполнить с помощью одной последовательности переходов, в графе имеется несколько несвязанных ветвей. Следовательно, в СЗИ есть ошибка, так как нельзя добиться, чтобы все функции безопасности выполнялись корректно без нарушения работы других функций безопасности. Поэтому в статье не рассматривается вариант с несколькими последовательными обходами графа СЗИ.

Таким образом, предложен подход к проверке выполнимости задачи тестирования произвольного программно-аппаратного СЗИ с использованием положений теории графов. В соответствии с данным подходом для некоторых программно-аппаратных средств защиты эту задачу решить невозможно (не все вершины графа принадлежат орцепи или компоненте сильной связности). Для остальных СЗИ задача имеет решение в худшем случае за полиномиальное время с использованием известных алгоритмов на графах.

В качестве развития проведенного исследования можно предложить изменение задачи тестирования путем включения в нее негативного тестирования, т. е. проверки невыполнимости функций безопасности в состояниях $V_{\text{ФБ}} \setminus V$. Подходы и алгоритмы решения такой задачи тестирования будут полностью аналогичными за исключением необходимости их применения ко всему графу $G_m$, а не к производному графу $G'_m$, полученному после исключения ненужных для изначальной задачи тестирования вершин и дуг.

**Литература**


1. *Beizer B.* Software testing techniques, 2nd ed. — Dreamtech, 2003.
2. *Broy M., Jonsson B., Katoen J. P., Leucker M., Pretschner A.* Model based testing of reactive systems. — LNCS 3472, Springer Berlin Heidelberg, 2005.
3. *Кулямин В. В.* Тестирование на основе моделей. Курс лекции ВМиК МГУ [Электронный ресурс]. URL: http://panda.ispras.ru/~kuliamin/mbt-course.html (дата обращения: 29.05.2021).
4. *Бурдонов И. Б., Косачев А. С., Кулямин В. В.* Использование конечных автоматов для тестирования программ // Программирование. 2000. № 2. С. 12—28.
5. *Kanner T. M.* Applicability of software testing methods to software and hardware data security tools // Glob. J. Pure Appl. Math. 2016. V. 12(1). P. 167—190.
6. *Kanner A. M., Kanner T. M.* Testing Software and Hardware Data Security Tools Using the Automata Theory and the Graph Theory: Proceedings of Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology. 2020. P. 615—618.
7. *Седжвик Р.* Фундаментальные алгоритмы на С. Ч. 5: Алгоритмы на графах. Изд. 3. — СПб.: ДиаСофтЮП, 2003. — 496 с.
8. *Edmonds J., Johnson E. L.* Matching Euler tours and the chinese postman // Mathematical programming. 1973. V. 5(1). P. 88—124.
9. *Скиена С. С.* Алгоритмы. Руководство по разработке. Изд. 2. / Пер. с англ. — СПб.: БХВ-Петербург, 2018.
10. *Кормен Т. и др.* Алгоритмы: построение и анализ. Изд. 3. — М.: Вильямс, 2013. — 1328 с.
11. *Sharir M.* A strong connectivity algorithm and its applications to data flow analysis // Computers and Mathematics with Applications. 1981. V. 7(1). P. 67—72.


# Algorithm for testing security functions of software and hardware data security tools based on the use of the graph theory


*T. M. Kanner*
JSC "OKB SAPR", Moscow, Russia



*The article discusses existing approaches to testing software and hardware data security tools (DST), which allow to ensure the completeness of testing, but do not solve the issue of its optimality. The definition of the problem of testing software and hardware DST is given and an approach to checking its feasibility using graph theory is proposed. The algorithm based on this approach is considered for testing security functions of software and hardware DST, which makes it possible to ensure its completeness and optimality.*



*Keywords:* software and hardware DST testing, completeness and optimality of testing, directed loop-free graph without multiple edges, algorithm for testing security functions of software and hardware DST, Chinese postman problem, Eulerian path.

Bibliography — 11 references. *Received July 1, 2021*

УДК 004.056.52
DOI: 10.52190/2073-2600_2021_3_16

# Формирование механизма присвоения доверия и разграничения прав доступа к информационным ресурсам предприятия

*А. М. Трошков*, канд. техн. наук; *А. Н. Ермакова*, канд. эконом. наук;
*С. В. Богданова*, канд. пед. наук
ФГБОУ ВО «Ставропольский государственный аграрный университет», г. Ставрополь, Россия

*Определены основные процедуры, уровни присвоения доверия пользователям информационной системы предприятия и категории защиты корпоративных информационных ресурсов, что стало основой для разработки структуры механизма управления доступом к данным и проектирования алгоритма разграничения доступа к ним с учетом статуса и грифованности информации.*

*Ключевые слова:* информационная безопасность, конфиденциальность, доверие, управление информационной системой, информационные ресурсы.

Большое количество предприятий с различной формой собственности формирует свою политику информационной безопасности, основным сегментом которой является конфиденциальность. Цель исследования — раскрытие роли информационной безопасности через решение такой задачи, как разработка механизма управления доступом к данным предприятия и алгоритма разграничения доступа к ним.

## Методология

Основными методами исследования послужили анализ и теоретический синтез, которые позволили систематизировать знания о цифровой конфеденции, её основных процедурах, уровнях присвоения, категориях защиты корпоративных информационных ресурсов. Они стали объективной основой для выдвижения гипотезы о необходимости разработки алгоритма и механизма управления доступом к информационным ресурсам предприятия.

## Результаты

При проведения анализа методологических контуров информационной безопасности, под цифровой конфиденцией будем понимать согласованное доверие относительно обработки, передачи и хранения информационных ресурсов, циркулирующих в системе электронного документооборота, между допущенными должностными лицами и другими
несогласованными пользователями. Под обозначенными информационными ресурсами понимаются устные или документированные сведения, не подлежащие всеобщей огласке, предполагаемые к обороту в особо доверительной, откровенной или секретной обстановке и представляющие определенную ценность.

Определение степени доверия к пользователям — это совокупность представлений и настроений субъекта информационных отношений:

- отражающих его ожидания, что пользователь будет реализовывать динамику функционирования элементов, сохраняющую плановые мероприятия информационной безопасности;
- проявляющихся как желание пользователя делегировать ряд полномочий в реализации функций управления конфиденциальной информацией [1].

Мониторинг современных подходов к формированию политики информационной безопасности предприятий позволяет иллюстрировать информационный инструментарий доверия следующим образом (рис. 1).

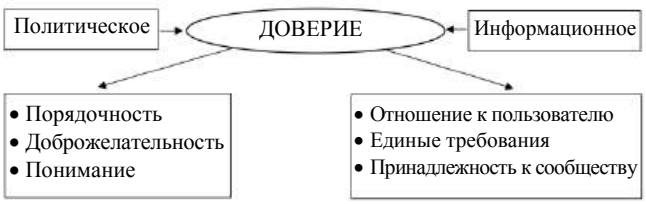



***Рис. 1. Схема организационного механизма функционирования доверия***

**Трошков Александр Михайлович**, доцент, доцент кафедры "Информационные системы".
E-mail: troshkov1954@mail.ru
**Ермакова Анна Николаевна**, доцент, доцент кафедры "Информационные системы".
E-mail: dannar@list.ru
**Богданова Светлана Викторовна**, доцент кафедры "Информационные системы".
E-mail: svetvika@mail.ru

*Статья поступила в редакцию 21 июля 2021 г.*

© Трошков А. М., Ермакова А. Н., Богданова С. В., 2021

Противоположность доверия — недоверие, которое характеризует информационный процесс с математической точки зрения как отказывающий фактор в предоставлении полномочий управления доступом к информационным ресурсам.

Недоверительность по своей технологической природе показывает степень лояльности отношения к пользователю информации и определяет возможность делегирования части должностных обязанностей при согласии стороннего пользователя соблюдать заданные требования информационной безопасности.

Основой каждой политики информационной безопасности является формирование информационных сегментов по уровню присвоения грифа конфиденциальности и мандатному присвоению степени доверия к сотрудникам, что позволяет разграничивать права доступа в соответствии со следующими процедурами (рис. 2).

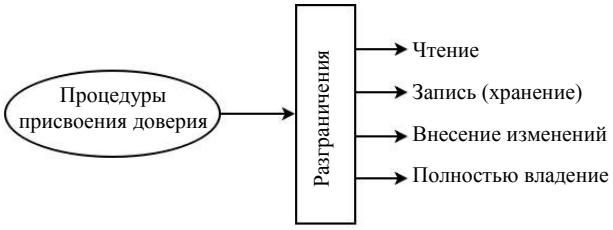



***Рис. 2. Процедуры присвоения доверия***

Предлагаемые процедуры позволяют, с одной стороны, осуществлять полный анализ разграничения на корректность и полноту, а с другой — реализовывать в дальнейшем полную систему многоэшелонной защиты информационного облака с данными о функционировании предприятия [2]. Прежде чем присвоить уровень доверия, необходим классификационный подход к объектам (сегментам) защиты, который обеспечит санкционный доступ к управлению информационной системой. Все объекты защиты информационных ресурсов вне зависимости от способа их представления и обработки сжато могут быть представлены в виде достаточной необходимости в них. Статус пользователей обязательно учитывается в процедуре присвоения уровня и категории объектов защиты (рис. 3).

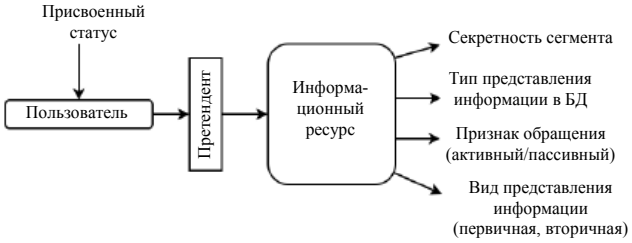



***Рис. 3. Категории уровня защиты***

Самое сложное в проектировании алгоритма — это анализ, выделение сегментов, статус пользователя, доступ [3]. Исходя из этого проектируемый алгоритм представлен на рис. 4.


***Рис. 4. Проектируемый алгоритм и его структура по управлению доступом***

Разработанный алгоритм позволяет сформировать структуру связанных между собой уровней информационных требований пользователей с учетом их статуса и грифованности информации предприятий.

## Заключение

Предложенные в исследовании процедуры позволяют осуществлять правильный и качественный мониторинг руководителям, формирующим политику безопасности предприятий. В целом весь алгоритм дает оптимальную картину управления и разграничения доступа, так как учитывает все особенности работы с сегментами информации.

**Литература**

1. *Гарфинкель Г.* Концепция и экспериментальные исследования "доверия" как условия стабильных согласованных действий / Пер. с анг. А. М. Корбута // Социологическое обозрение. 2009. Т. 8. № 1. С. 10—51.

2. *Трошков А. М., Трошков М. А.* Концепция проектирования биометрической системы для управления допуском к информационным ресурсам // Вестник СевКавГТИ. 2012. № 13. С. 16—20.

3. *Асанов С. М., Кузнецов А. Э., Тарасюк М. В.* Технология построения АС с многоуровневым доступом для государственных и правительственных структур РФ // Защита информации. Конфидент. 2003. № 6. С. 28.

# Formation of a mechanism for assigning trust and differentiating access rights to information resources of an enterprise

*A. M. Troshkov, A. N. Ermakova, S. V. Bogdanova*
Stavropol State Agrarian University, Stavropol, Russia

*This study defines the main procedures, the levels of assigning trust to users of the enterprise information system and the category of protection of corporate information resources, which became the basis for developing the structure of a mechanism for controlling access to data and designing an algorithm for delimiting access to them, taking into account the status and identification of information.*

*Keywords*: information security, confidentiality, the trust, information system management, informational resources.

Bibliography — 3 references. *Received July 21, 2021*

УДК 004.056.2
DOI: 10.52190/2073-2600_2021_3_19

# Контроль целостности образов виртуальных машин на платформе OpenStack

*Д. О. Стасьев*
Московский физико-технический институт (национальный исследовательский университет), г. Долгопрудный, Московская обл., Россия

*Определен формат, используемый для контроля целостности (КЦ) образов и конфигураций образов виртуальных машин (ВМ) путем их сравнения, в состав которого входят данные из набора таблиц из Glance DB (OpenStack Glance — компонент, созданный для управления образами ВМ). Описаны события взаимодействия разрабатываемого модуля с эталоном. Результатом работы стала архитектура программного модуля, реализующего проверку конфигураций образов ВМ на соответствие с эталоном.*

*Ключевые слова:* виртуализация, виртуальная машина, OpenStack, Glance, образы виртуальных машин, целостность, контроль целостности, обеспечение целостности, компоненты виртуальных машин, программный модуль.

Согласно аналитическому исследованию [1], проведённому компанией "Код Безопасности" в 2018 г. среди 305 участников (IT-директора, ведущие инженеры, специалисты по защите информации, руководители направлений информационной безопасности), значительная часть организаций, независимо от масштабов их бизнеса, использует виртуализацию в серверной инфраструктуре более чем на 50 % серверов. Применение данной технологии позволяет эффективно использовать вычислительные мощности оборудования, сокращает время его простоя, однако создаёт опасность — появляется дополнительный канал для проникновения злоумышленника, повышается вероятность потери конфиденциальных данных, обрабатываемых на серверах с виртуализацией 70 % российских компаний-респондентов. Поэтому несмотря на то, что в среднем только 38 % российских компаний опасается действий злоумышленника, актуальность рассмотрения вопросов обеспечения безопасности при использовании виртуализации остаётся высокой.

Например, OpenStack, являясь одной из популярных платформ для создания виртуальных инфраструктур (ВИ — это система, которая обеспечивает поддержку виртуализации серверов, сети и хранилищ данных, создаётся с помощью инфраструктуры виртуализации), не предоставляет надёжных механизмов контроля целостности ВИ и создаваемых в ней виртуальных машин (ВМ). Только в 2015 г. в OpenStack начали внедрять защитные функции, такие, как, например, КЦ образов ВМ [2]. Для его реализации изначально стали использовать подпись (RSA-PSS) контрольной суммы, вычисленной от данных образа ВМ с помощью алгоритма хеширования MD5, который не является криптографически стойким. Отсутствие криптостойкости позволяло злоумышленнику заменить исходный образ ВМ на произвольный (злоумышленник мог добиться коллизии между значениями хеш-функции от исходного образа и произвольного). В 2016 г. от контрольной суммы отказались, заменили её вычислением подписи от содержимого образа напрямую [3]. Однако несмотря на это, в OpenStack оставались критические уязвимости. Например, в случае несовпадения хранимой и заново вычисленной подписей платформа выводила сообщение (в логах ошибок) о невозможности создания ВМ, содержащее требуемое значение подписи. Злоумышленник, получив информацию о требуемом для создания образа значении подписи, получал возможность так заменить значение подписи для своего образа в базе данных (БД), что создание ВМ из его образа не блокировалось системой. Иными словами, злоумышленник получал возможность создавать ВМ из произвольного образа, потенциально содержащего программные закладки или любое другое вредоносное программное обеспечение [4].

Несмотря на активное развитие OpenStack и исправление ошибок, в платформе продолжают находить уязвимости, которые создают угрозы различных уровней [5]. Таким образом, кроме использования встроенных в OpenStack механизмов защиты от злоумышленников, необходимо использовать дополнительные наложенные средства защиты информации (СЗИ).

**Стасьев Денис Олегович**, студент.
E-mail: stasev.do@phystech.edu

*Статья поступила в редакцию 29 июля 2021 г.*

© Стасьев Д. О., 2021

## Используемые методы исследования

При создании СЗИ для КЦ ВМ в OpenStack-based ВИ необходимо реализовывать мониторинг не только целостности критических файлов самих ВМ, но и метаданных образов ВМ (хранятся в отдельной БД в OpenStack). В свою очередь, только КЦ ВМ (в том числе образов ВМ) недостаточно для осуществления полноценного КЦ всей OpenStack-based ВИ. Необходимо дополнительно обеспечивать КЦ конфигурации (связи в графе конфигурации ВИ [6]) и компонентов ВИ [7]. Таким образом, КЦ OpenStack-based ВИ — комплексная задача, для решения которой необходим мониторинг целостности как отдельных компонентов ВИ, так и связей между ними.

Данная статья посвящена решению одной из частей описанной задачи КЦ ВМ в OpenStack — КЦ конфигураций образов ВМ. Для этого будет разработана архитектура программного модуля, реализующего КЦ.

Для разработки механизма внедрения модуля в OpenStack-based ВИ необходимо определить компоненты OpenStack, участвующие во взаимодействии с ВМ. Для этого из официальной документации OpenStack с помощью метода абстрагирования выделяются компоненты OpenStack для создания ВИ. Системный анализ полученных данных позволит определить компоненты OpenStack и их части, участвующие во взаимодействии с ВМ. С помощью применения такого эмпирического метода, как описание, изучается строение БД Glance DB для формирования структуры эталона конфигурации образа ВМ. Результатом работы станут архитектура программного модуля, реализующего КЦ, а также описание некоторых особенностей её реализации.

## Обзор литературы

*Компоненты OpenStack, участвующие во взаимодействии с ВМ.* Перед исследованием особенностей платформы OpenStack введём основные понятия в области серверной виртуализации. Гипервизор — программа и/или аппаратная система, обеспечивающая одновременное, параллельное выполнение нескольких сред (каждая среда обычно является программной системой, содержит операционную систему (ОС) и эмулирует аппаратное обеспечение некоторой target-платформы) на одном хост-компьютере (host-платформе). Экземпляром ВМ (или просто ВМ) будем называть отдельную среду, которую можно получить с помощью гипервизора. Образом ВМ именуем совокупность файлов (может состоять из одного), используемую в качестве шаблона (образца) при создании новых экземпляров ВМ.

OpenStack — это система, состоящая из комплекса программного обеспечения (ПО), созданная для управления большими наборами вычислительных ресурсов, хранилищ и сетевых ресурсов [8]. Платформа OpenStack предоставляет архитекторам ВИ набор компонентов (сервисов), с помощью которых можно разработать архитектуру и создать требуемую ВИ, управлять как состоянием ВМ, так и аппаратными ресурсами.

Можно выделить несколько сервисов, которые созданы в OpenStack для взаимодействия с ВМ. OpenStack Glance используют для управления образами (шаблонами) ВМ (например, для добавления и удаления образов). Созданием ВМ из образов занимается сервис OpenStack Nova (рис. 1).

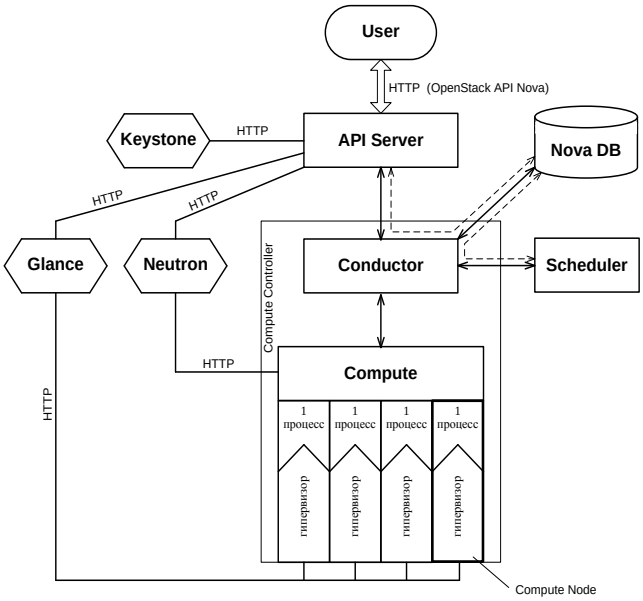



***Рис. 1. Схема взаимодействия частей OpenStack Nova***

При создании ВМ Nova обращается к Glance, который получает образ из какого-либо хранилища. Сервис Nova, кроме создания экземпляров ВМ, позволяет ими управлять [9]. Например, можно менять аппаратные ресурсы ВМ с помощью применения (смены) готовых конфигураций (содержат размер доступной оперативной и постоянной памяти экземпляру ВМ), называемых flavor. Также Nova позволяет выбрать и настроить гипервизоры для ВМ. Сами файлы образов и экземпляров ВМ находятся в отдельном хранилище. В зависимости от конфигурации OpenStack-based ВИ тип и реализация хранилища могут быть разными: в самом простом случае это может быть файловая система хост-компьютера, однако на практике часто используют специальные сервисы OpenStack, реализующие хранилища (OpenStack Swift, Open-

Stack Cinder) [10, 11]. Для аутентификации и авторизации пользователей в OpenStack используется сервис Keystone. Под пользователями в нём понимают как людей, работающих непосредственно с ВИ (например, администраторов и архитекторов ВИ), так и сервисы OpenStack, между которыми происходит взаимодействие. Рассматриваемые сервисы OpenStack (Glance, Nova, Keystone) реализованы как один либо как набор web-серверов, поэтому взаимодействие с ними и между ними происходит с помощью HTTP-запросов с соответствующими заголовками (для Keystone).

*Хранение образов ВМ и их конфигураций в OpenStack.* Жизненным циклом ВМ будем называть совокупность процессов и состояний системы, связанных с созданием, использованием, хранением и удалением экземпляров ВМ. Для обеспечения целостности ВМ необходим КЦ на всех этапах жизненного цикла ВМ. Первым этапом жизненного цикла ВМ является её создание из образа ВМ.

OpenStack предоставляет широкие возможности по взаимодействию с образами ВМ с помощью сервиса Glance. Рассмотрим его подробнее. Glance (Image service) — компонент, созданный для управления образами ВМ и метаданными ВИ [12, 13]. Под метаданными понимают элементы ассоциативного массива (пары ключ—значение), которыми могут управлять администраторы ВИ (например, создавать, удалять, применять к образам ВМ). До применения метаданных к конкретным ресурсам OpenStack они не влияют на ВИ, но после добавления метаданных к различным объектам OpenStack объекты могут использовать метаданные как источник настроек, т. е. метаданные могут влиять на конфигурацию частей ВИ.

Сервис Glance состоит из большого числа внутренних подсистем [14]. С помощью применения метода абстрагирования можно выделить четыре основные части, представленные на рис. 2: Glance API Server, Glance Registry, Glance DB (каталог метаданных) и хранилище образов и файлов ВМ. Glance Registry является основной частью Glance, предоставляет Glance API Server информацию о наличии образов в Glance и об их расположении в хранилище с помощью Glance DB. Glance DB является БД, которая содержит метаданные и расположение каждого образа в хранилище. Обычно для Glance DB используют реляционную БД, созданную на основе таких систем управления БД (СУБД), как MySQL и SQLite (являются наиболее популярными СУБД для OpenStack) [13—15]. Часто СУБД для Glance DB является единственной во всей OpenStack-based ВИ, поэтому она может использоваться и другими сервисами (обычно создаётся новый пользователь СУБД для отдельной требуемой БД для каждого сервиса; например, такой механизм реализован в OpenStack Nova). Образы ВМ, доступные через Glance, могут храниться в самых разных местах, от простых файловых систем до систем хранения, таких, как проекты OpenStack Swift, OpenStack Cinder или S3 [12]. Для работы Glance необходим сервис Keystone.

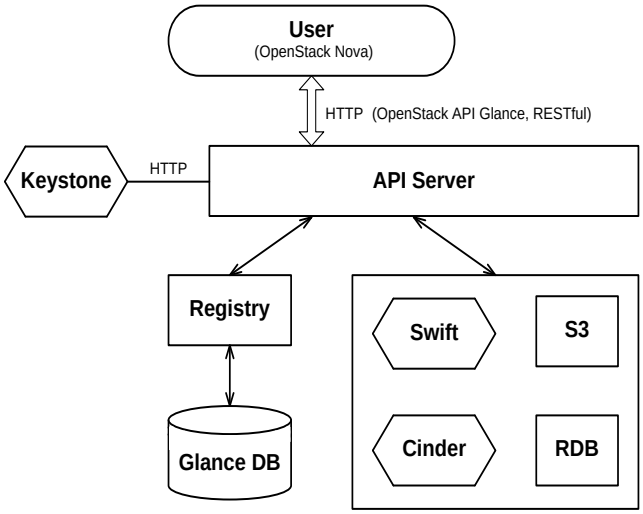



***Рис. 2. Схема взаимодействия частей OpenStack Glance***

*Glance DB и эталон конфигурации образа ВМ.* Для КЦ ВИ необходим, в частности, КЦ образов ВМ и их конфигураций, хранимых в Glance DB. Для КЦ самих образов, находящихся в хранилище, требуется вычислять контрольные суммы от содержимого файлов. Исследуем Glance DB, где хранятся метаданные и свойства образов ВМ. Можно объединить таблицы в несколько групп в соответствии с их ролями во взаимодействии с образами ВМ (таблица).

**Связь таблиц БД Glance и их ролей во взаимодействии с образами ВМ**

| Роль во взаимодействии с образами ВМ | Таблицы |
|---|---|
| Используются для миграций (SQLAlchemy) | 1. alembic_version<br>2. migrate_version |
| Содержат информацию о хранимых образах ВМ | 3. image_locations<br>4. image_members<br>5. image_properties<br>6. image_tags<br>7. images |
| Используются для обработки "больших" образов ВМ сервисом Glance [16] | 8. task_info<br>9. tasks |
| Необходимы для хранения метаданных [17] | 10. metadef_properties<br>11. metadef_tags<br>12. metadef_resourse_types<br>13. metadef_objects<br>14. metadef_namespaces<br>15. metadef_namespace_resource_types |

После определения ролей таблиц БД Glance во взаимодействии с образами ВМ можно перейти к вопросам КЦ образов ВМ. КЦ предполагает сравнение текущего состояния системы с некоторым его выбранным фиксированным состоянием, принятым за эталон [18]. После задания эталона в определённые моменты времени происходит сравнение актуального состояния системы с записанным в эталон. Наличие таких механизмов позволяет контролировать целостность системы [19]. В случае КЦ образов и метаданных образов ВМ в эталон образа ВМ должны входить поля таблиц (3)—(7), для КЦ метаданных всей ВИ — таблиц (10)—(15).

Поскольку рассматривается разработка механизма КЦ конфигураций образов ВМ, эталон конфигураций образов ВМ должен включать поля таблиц (3)—(7). Для вычисления значения эталона в данной работе будут использованы идентификатор образа ВМ (GUID, Globally Unique Identifier) (поле id таблицы images (7) БД Glance) и значение хеш-функции (контрольная сумма) от значений таблиц (3)—(7). В будущем предполагается, что данные пары будут храниться в аппаратно-защищённой области постоянной памяти. Для дополнительной защиты можно использовать идею патента [20] после согласования с патентообладателем: вычислять контрольную сумму не только от хранимых данных, но и от контрольной суммы предыдущей записи и ключа хранения, используемого программным модулем для подписи записываемых значений. Согласно патенту, можно использовать криптографию с открытым ключом, в которой подписывающее лицо (программный модуль) вычисляет контрольную сумму проверки целостности с помощью своего закрытого ключа, а лицо, желающее проверить целостность, может использовать свой открытый ключ для верификации. Вычисленная контрольная сумма присоединяется к записи данных [20].

Таким образом, поскольку разрабатывается механизм КЦ конфигураций образов ВМ, эталон образа ВМ должен включать значения таблиц (3)—(7) БД Glance.

## Результаты

*Архитектура программного модуля.* Описание внутреннего устройства OpenStack позволило выделить компоненты OpenStack, участвующие во взаимодействии с ВМ. Одним из них является система хранения образов ВМ и их конфигураций — OpenStack Glance. После изучения её устройства был установлен формат эталона конфигурации образа ВМ. Однако для реализации программного модуля для КЦ только описания эталона недостаточно. Необходимо также разработать архитектуру модуля, учитывая особенности платформы OpenStack.

Опишем предполагаемую архитектуру программного модуля. Её функционирование будет основано на вычислении эталона образа ВМ и его хранении в памяти хост-компьютера. В некоторые моменты времени функция в разрабатываемом модуле для создания эталона будет заново вычисляться и полученное значение будет сравниваться с записанным в память эталоном. В случае несовпадения вычисленного значения и эталона администратор ВИ будет получать уведомление о нарушении КЦ конфигураций образов ВМ. Система должна запрещать создание ВМ из образов при нарушении КЦ конфигураций образов при своих ошибках, например при отсутствии возможности получения данных из БД для вычисления образа.

Модуль должен запускаться до старта ВИ, чтобы создавать эталоны для всех добавляемых образов ВМ в ВИ. Определим, в какие моменты времени (в ответ на какие события) система должна вычислять эталоны. Изначально при добавлении образа ВМ в ВИ необходимо создавать исходные эталоны и помещать их в файл (возможно применение аппаратно-защищённой области памяти для хранения файла). При попытке создания экземпляра ВМ из образа ВМ эталон должен заново вычисляться и сравниваться с записанным в файл. Дополнительно образ используется при запуске созданной ВМ.

Определим, как отслеживать необходимые для КЦ конфигураций образов ВМ события (добавление образа ВМ в ВИ, создание экземпляра ВМ из образа и запуск ВМ) в платформе OpenStack.

Для определения момента запуска KVM-based ВМ можно использовать libvirt. Libvirt — это наиболее часто используемый драйвер виртуализации в OpenStack [21]. OpenStack Nova для работы с ВМ использует libvirt при поддержке программы QEMU (для эмуляции аппаратного обеспечения различных платформ) и, если доступен, KVM. Libvirt является свободной реализацией API-гипервизора KVM и содержит набор дополнительных возможностей [22]. Одной из них являются хуки. Это скрипты, позволяющие изменить стандартное поведение компонентов системы. Libvirt позволяет запускать пользовательские хуки на определённые события libvirt, например на запуск ВМ (/etc/libvirt/hooks/qemu) [23]. При выполнении хука libvirt передаёт ему некоторые параметры через аргументы командной строки. В зависимости от них можно понять статус

(например, запуск или остановка ВМ) и имя ВМ. То есть создав подобный хук, можно отслеживать запуск ВМ и инициировать проверку КЦ образа ВМ непосредственно перед запуском ВМ. Подобная идея успешно реализуется в специальном программном обеспечении (СПО) СЗИ от несанкционированного доступа (НСД) "Аккорд-KVM" компании "ОКБ САПР" [24]. В случае нарушения КЦ администратор будет получать оповещение. Таким образом, использование хуков libvirt для отслеживания запуска ВМ является наилучшим решением для отслеживания событий запуска ВМ и её создания из образа среди встраивания во внутреннюю очередь сообщений OpenStack Nova и прокси-сервера обработки запросов к Nova.

Теперь, зная имя запускаемой ВМ, необходимо получить образ, для которого требуется посчитать эталон. Поскольку информация о ВМ хранится в части Nova DB сервиса OpenStack Nova, исследуем этот компонент в целях нахождения информации о взаимосвязи между полем id таблицы images БД Glance (GUID) и названием запускаемой ВМ. Получаем, что в БД Nova содержится таблица instances с интересующей информацией. В ней хранятся метаданные созданных ВМ в OpenStack-based ВИ, такие, как статус, количество выделенной памяти, имя хост-компьютера и т. д. С помощью полей hostname (display_name) и image_ref устанавливается взаимосвязь между именем ВМ и используемым образом ВМ. Используя эту таблицу, можно установить соответствие между именем запускаемой ВМ, которое передаётся хуку libvirt в качестве аргумента командной строки, и образом ВМ, для которого необходимо посчитать эталон.

Установлено, как проверять соответствие образа ВМ хранимому эталону. Перейдем к тому, как и когда создавать исходный эталон. Необходимо создавать исходный эталон для каждого образа ВМ в момент его добавления в OpenStack-based ВИ. Поскольку OpenStack Glance управляет хранением образов ВМ, рассмотрим его устройство подробнее. В отличие от OpenStack Nova он не содержит нескольких внутренних серверов. Glance написан на Python и является HTTP-сервером. Его структура (схема) реализована через набор файлов-компонентов, каждый из которых обрабатывает запрос и направляет следующему [25]. То есть Glance состоит из набора "слоёв", каждый из которых реализует определённые функции и отправляет запрос на следующий "слой". Для определения момента добавления образа ВМ можно использовать прокси-сервера для обработки запросов к самой БД. Данный способ позволит создавать исходный эталон сразу после добавления записей в БД. Ещё одним его преимуществом является удобство конфигурирования, поскольку при его внедрении необходимо только изменить настройки БД в Glance (без изменения других сервисов OpenStack).

Таким образом, установлены события (моменты времени), в которые будет происходить взаимодействие разрабатываемого программного модуля с эталонами конфигурации образов ВМ. Разработаны способы внедрения в OpenStack: выбраны использование хуков libvirt для определения момента запуска ВМ и прокси-сервер для БД Glance для определения момента добавления образов ВМ в сервис OpenStack Glance.

*Практические аспекты реализации архитектуры модуля*. Разрабатываемая система должна внедряться на хост-компьютер ВИ, иметь доступ к сервисам OpenStack и предоставлять удобный способ управления настройками КЦ конфигураций образов ВМ. При создании системы можно использовать клиент-серверную архитектуру. Сервер будет запускаться на хост-компьютере ВИ до старта ВИ и принимать HTTP-запросы (от хука libvirt), которые вызовут либо добавление эталона в память, либо проверку КЦ конфигурации образа ВМ. Клиентом может являться веб-приложение, которое по протоколу WebSocket будет получать сообщение и уведомлять администратора в случае нарушения КЦ. Сервер в таком случае должен запрещать запуск ВМ. Ещё одной частью системы будет хук libvirt, который при вызове отправит соответствующий HTTP-запрос на сервер в целях его уведомления о необходимости проверки КЦ образа запускаемой ВМ. Получив запрос, сервер обратится в БД Nova и определит идентификатор образа ВМ. Используя его, сервер вычислит эталон от значений таблиц БД Glance и сравнит значение с хранимым в памяти. В случае несовпадения значений сервер отправит широковещательное сообщение по WebSocket о нарушении КЦ конфигурации образа ВМ (сообщение получит администратор ВИ с установленным соединением). Подробная схема взаимодействия представлена на рис. 3.

Для создания исходных эталонов в памяти прокси-сервер БД Glance будет обрабатывать запросы в БД Glance. В случае запросов создания (изменения) образов ВМ будет вычисляться и сохраняться эталон. Подробная схема создания эталонов конфигураций образов ВМ представлена на рис. 4.

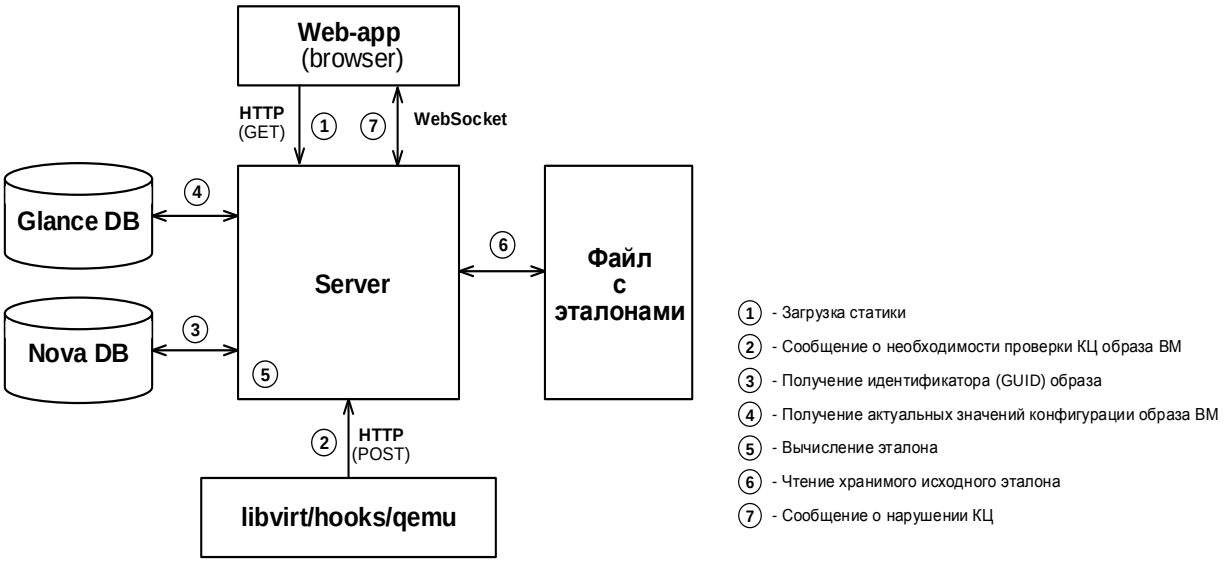



***Рис. 3. Схема проверки КЦ конфигураций образов ВМ***

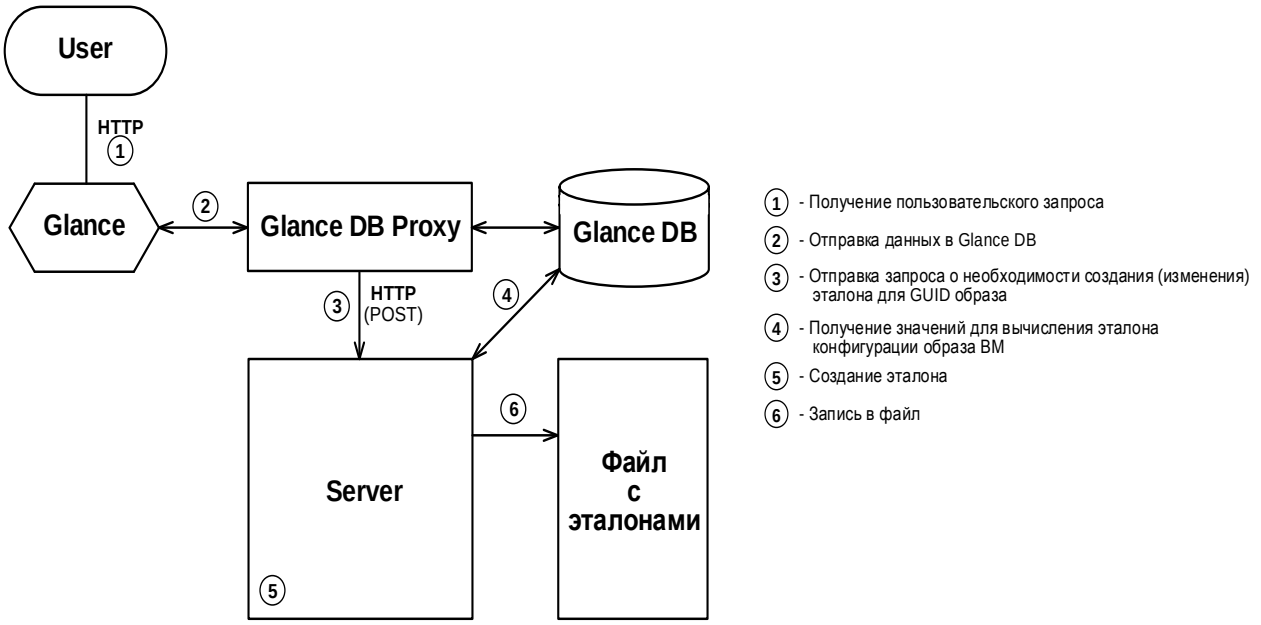



***Рис. 4. Схема создания эталонов образов ВМ***

## Обсуждение

В платформе OpenStack для отслеживания необходимых для КЦ конфигураций образов ВМ событий помимо выбранных подходов (хуки libvirt для определения момента запуска ВМ и прокси-сервер для БД Glance для определения момента добавления образов ВМ) можно использовать и другие.

Старт ВМ и её создание из образа происходят с помощью обработки соответствующих запросов сервисом OpenStack Nova. Поскольку Nova является совокупностью нескольких сервисов, общающихся с помощью очереди сообщений RabbitMQ, можно читать эти сообщения (т. е. можно встроить модуль в сам сервис Nova). Однако формат этих сообщений строго не определён (поскольку является внутренней служебной частью сервиса). Поэтому существует риск возникновения проблем с совместимостью разрабатываемого СЗИ с новыми версиями платформы OpenStack. Поскольку OpenStack активно развивается и выпускает несколько релизов в год, потенциальные затраты на поддержание работоспособности такого СЗИ высоки.

Кроме того, очередь сообщений обрабатывает большое количество запросов между внутренними сервисами OpenStack Nova. Поэтому система для их чтения будет требовать значительных ресурсов.

Другим решением для определения момента запуска ВМ может стать создание прокси-сервера для обработки запросов к OpenStack Nova. Упрощённо Nova API Server (часть OpenStack Nova, см. рис. 1) можно считать HTTP-сервером. Взаимодействие между пользователем и Nova (и между другими сервисами OpenStack и Nova) основано на взаимодействии через публичное API. Оно хорошо документировано, т. е. на его основе можно разработать прокси-сервер со специальной обработкой некоторых запросов (здесь для вычисления эталона). Настроив конфигурации остальных сервисов OpenStack-based ВИ, возможно внедрить такой сервер в структуру OpenStack. Одной из проблем будет возможность различить легальных пользователей и нарушителей, поскольку необходимо обрабатывать запросы в соответствии с правами пользователей. Для этого потребуется отдельно настроить взаимодействие прокси-сервера с сервисом OpenStack Keystone (в случае возникновения проблем с настройкой можно заменить OpenStack Keystone собственным сервисом аутентификации и авторизации, однако целесообразность разработки такого решения вызывает вопросы, так как сервис необходимо будет адаптировать к взаимодействию со всеми сервисами OpenStack). Ещё одной проблемой может стать относительно большая задержка между проверкой КЦ конфигурации образа и запуском ВМ, поскольку после проверки КЦ запрос будет отправляться в другой сервис. Предложенное решение (из-за своей архитектуры: отправки запроса в другой сервис) не позволит существенно снизить задержку. Необходимо осуществлять проверку КЦ непосредственно перед запуском ВМ. Этого можно достичь с помощью хуков libvirt, как было выбрано в описанной ранее архитектуре программного модуля.

Для определения момента добавления образа ВМ существует несколько способов, кроме выбранного (прокси-сервер для БД Glance). Аналогично рассмотренному решению для OpenStack Nova можно сделать прокси-сервер для обработки запросов к Glance. В момент получения ответа от Glance прокси-сервер будет создавать исходный эталон. Однако возникает проблема, связанная с относительно большой задержкой между фактическим созданием записей в Glance DB и вычислением эталона. Другой способ — создание дополнительного слоя для Glance, который будет создавать эталон непосредственно до создания записей в БД. Однако это требует внедрения во внутреннюю структуру Glance, что усложнит поддержку разрабатываемого программного модуля при появлении новых версий OpenStack.

В заключение можно отметить, что особенностью разработанной архитектуры программного модуля для КЦ конфигураций образов ВМ является возможность внедрения КЦ содержимого файлов образов ВМ без необходимости внесения значительных изменений в архитектуру СЗИ.

## Заключение

Получено решение одной из частей задачи КЦ ВМ в OpenStack — КЦ конфигураций образов ВМ. Описанная архитектура программного модуля реализует проверку конфигураций образов ВМ, хранимых в базе данных Glance DB платформы OpenStack, на соответствие эталону.

При развитии модуля для обеспечения КЦ конфигураций ВМ, хранимых в Nova DB, использование контрольных сумм в качестве эталона может оказаться не наилучшим вариантом, поскольку в отличие от образов для одной ВМ в системе значительно чаще может быть несколько разрешённых состояний. Данный вопрос необходимо исследовать отдельно. Возможным решением может стать применение атрибутных моделей контроля доступа к КЦ конфигураций ВМ [19].

**Литература**


1. Защита виртуальной инфраструктуры. Официальный сайт компании Код Безопасности [Электронный ресурс]. URL: https://www.securitycode.ru/upload/iblock/d0d/Virtualization_2018.pdf (дата обращения: 02.12.2020).

2. Image Signing and Verification Support: Blueprints: Glance [Электронный ресурс]. URL: https://blueprints.launchpad.net/glance/+spec/image-signing-and-verification-support (дата обращения: 02.12.2020).

3. OpenStack Docs: Glance Image Signing and Verification [Электронный ресурс]. URL: https://specs.openstack.org/openstack/glance-specs/specs/mitaka/implemented/image-signing-and-verification-support.html (дата обращения: 02.12.2020).

4. Glance Image creation checksum logic — Ask OpenStack: Q&A Site for OpenStack Users and Developers [Электронный ресурс]. URL: https://ask.openstack.org/en/question/90047/glance-image-creation-checksum-logic/ (дата обращения: 02.12.2020).

5. Bugs: Glance [Электронный ресурс]. URL: https://bugs.launchpad.net/glance/+bugs?field.tag=security (дата обращения: 02.12.2020).

6. *Мозолина Н. В.* Разработка средства контроля целостности виртуальной инфраструктуры и её конфигурации: выпускная квалификационная работа. 2017. С. 19—36.

7. *Мозолина Н. В.* Контроль целостности виртуальной инфраструктуры и ее конфигурации // Вопросы защиты информации. 2016. № 3. С. 31—33.

8. What is OpenStack? [Электронный ресурс]. URL: https://openstack.org/software (дата обращения: 02.12.2020).

9. *Журов П. М.* Разработка и исследование модели доступа к объектам облачных инфраструктур: выпускная квалификационная работа. 2019. С. 18—22, 77—81.

10. OpenStack Docs: Swift Architectural Overview [Электронный ресурс]. URL: https://docs.openstack.org/swift/latest/overview_architecture.html (дата обращения: 02.12.2020).

11. OpenStack Docs: OpenStack Block Storage (Cinder) documentation [Электронный ресурс]. URL: https://docs.openstack.org/cinder/latest/ (дата обращения: 02.12.2020).

12. OpenStack Docs: Welcome to Glance's documentation! [Электронный ресурс]. URL: https://docs.openstack.org/glance/latest/ (дата обращения: 02.12.2020).

13. OpenStack Docs: Glance database architecture [Электронный ресурс] URL: https://docs.openstack.org/glance/pike/contributor/database_architecture.html (дата обращения: 02.12.2020).

14. OpenStack Docs: Basic architecture [Электронный ресурс] URL: https://docs.openstack.org/glance/pike/contributor/architecture.html (дата обращения: 02.12.2020).

15. OpenStack Docs: Image service overview [Электронный ресурс] URL: https://docs.openstack.org/glance/latest/install/get-started.html (дата обращения: 02.12.2020).

16. OpenStack Docs: Tasks [Электронный ресурс]. URL: https://docs.openstack.org/glance/pike/admin/tasks.html (дата обращения: 02.12.2020).

17. OpenStack Docs: Using Glance's Metadata Definitions Catalog Public APIs [Электронный ресурс]. URL: https://docs.openstack.org/glance/pike/user/glancemetadefcatalogapi.html (дата обращения: 02.12.2020).

18. *Мозолина Н. В.* Задание эталона при контроле целостности конфигурации виртуальной инфраструктуры: сб. научных статей XII Междунар. науч.-техн. конф. "Новые информационные технологии и системы", Пенза. 23—25 ноября 2016. С. 219—225.

19. *Ерин Ф. М.* Построение шаблонов для решения задачи контроля целостности конфигурации на основе атрибутной модели контроля доступа // Вопросы защиты информации. 2018. № 3. С. 3—6.

20. *Миеттинен М., Хятёнен К.* Способ обеспечения целостности набора записей данных. Российский патент 2009 года RU 2351978 C2. Изобретение по МКП G06F11/08 [Электронный ресурс] URL: https://patenton.ru/patent/RU2351978C2_ (дата обращения: 02.12.2020).

21. OpenStack Docs: Libvirt — Nova Virtualisation Driver // Официальный сайт документации OpenStack [Электронный ресурс]. URL: https://docs.openstack.org/kolla-ansible/latest/reference/compute/libvirt-guide.html (дата обращения: 02.12.2020).

22. libvirt: Domain XML format [Электронный ресурс]. URL: https://libvirt.org/formatdomain.html (дата обращения: 02.12.2020).

23. libvirt: Hooks for specific system management [Электронный ресурс]. URL: https://libvirt.org/hooks.html (дата обращения: 02.12.2020).

24. Специальное программное обеспечение средств защиты информации от несанкционированного доступа "Аккорд-KVM". Руководство администратора безопасности информации [Электронный ресурс]. URL: https://www.okbsapr.ru/upload/iblock/786/786f40d485a08e160fca07f38fbd78e6.pdf (дата обращения: 02.12.2020).

25. OpenStack Docs: Glance domain model implementation [Электронный ресурс]. URL: https://docs.openstack.org/glance/latest/contributor/domain_implementation.html (дата обращения: 02.12.2020).

## Integrity control of virtual machine images on the OpenStack platform

*D. O. Stasyev*

Moscow Institute of Physics and Technology (National Research University), Dolgoprudny, Moscow region, Russia

*Despite the presence of built-in integrity control (IC) mechanisms, the OpenStack platform does not contain reliable solutions for IC of images and configurations of images of virtual machines (VM). For IC of configurations, it is necessary to use their comparison with some reference (standard). The article defines its format, includes a set of tables from Glance DB (OpenStack Glance is a component created for managing VM images). The events of interaction of the developed module with the reference are described. The result of the work is the architecture of a software module that checks the configurations of VM images for compliance with the reference.*

*Keywords:* virtualization, virtual machine, OpenStack, Glance, virtual machine images, integrity, integrity control, integrity assurance, virtual machine components, software module.

Bibliography — 25 references. *Received July 29, 2021*

# ДОВЕРЕННАЯ СРЕДА

УДК 004.056
DOI: 10.52190/2073-2600_2021_3_27

## Особенности моделирования угроз безопасности в системе Интернета вещей

[1] *П. А. Иванов*; [1, 2] *И. В. Капгер*, канд. техн. наук
[1] ФГБОУ ВО «Национальный исследовательский университет «МЭИ», Москва, Россия
[2] ФГБОУ ВО «Пермский национальный исследовательский политехнический университет», г. Пермь, Россия

*Рассматривается подход к моделированию угроз безопасности информации в системах Интернета вещей, учитывающий особенности взаимодействия устройств Интернета вещей между собой и с окружающими их компонентами. Предложен подход к моделированию угроз, подразумевающий рассмотрение угроз, направленных на ресурсы и компоненты системы, а также угроз, направленных на пользователя системы и окружающую среду.*

*Ключевые слова*: кибербезопасность, угрозы безопасности, моделирование угроз, Интернет вещей.

В качестве угроз безопасности в процессе моделирования рассматривают неправомерные действия и воздействия на информационные ресурсы или компоненты систем или сетей, в результате которых возможны нарушение безопасности информации, нарушение или прекращение функционирования систем и сетей. В общем случае при моделировании угроз учитывают тип информационной системы и её характеристики, возможные источники угроз и способы их реализации.

Для систем Интернета вещей (Internet of Things, IoT) моделирование угроз имеет ряд особенностей за счёт использования специфичной модели взаимодействия устройств, архитектуры информационных сетей, включающих устройства Интернета вещей, а также самих устройств: они ориентированы на взаимодействие с физическим миром, в особенности с человеком.

Концептуально системы Интернета вещей представляют собой информационные системы, включающие устройства ("вещи"), оснащенные встроенными технологиями для взаимодействия друг с другом и с внешней средой. На рис. 1 представлена типовая архитектура системы Интернета вещей.

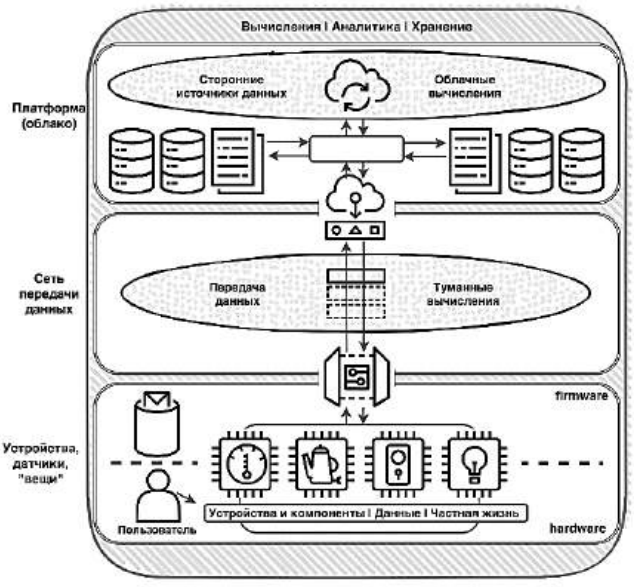



***Рис. 1. Архитектура системы Интернета вещей***

Ориентация устройств Интернета вещей в процессе выполнения их бизнес-функций на взаимодействие с физическим миром и человеком, а также фактическое выделение функций по управлению, обеспечению безопасности и защиты конфиденциальности во второстепенную "вспомогательную" подгруппу служат причиной появле-

**Иванов Павел Алексеевич**, магистр.
E-mail: pashaivan17@gmail.com
**Капгер Игорь Владимирович**, доцент кафедры "Безопасность и информационные технологии", доцент кафедры "Автоматика и телемеханика".
E-mail: Kapger@mail.ru

*Статья поступила в редакцию 9 июля 2021 г.*

© Иванов П. А., Капгер И. В., 2021

ния различных каналов реализации угроз и представляют основной интерес с точки зрения потенциального воздействия на состояние защищенности и нарушение конфиденциальности.

С учётом данных положений при определении и классификации угроз безопасности следует исходить из того, что IoT-устройства обладают функциональными возможностями, отличными от ИТ-устройств, которые реализуются ими самостоятельно или при взаимодействии с другими сторонними объектами или субъектами. К ним относятся возможности:

- взаимодействия с физическим миром путем преобразования информации;
- интеграционных взаимодействий типа "устройство—устройство" и "устройство—человек";
- обеспечения поддержки функционирования.

Указанные особенности не позволяют рассматривать только угрозы, для которых объектами неправомерных воздействий являются ресурсы и компоненты систем и сетей. Требуется рассмотрение угроз, направленных на человека (как пользователя системы и как его компонента), а также среду, в которой функционирует IoT-система. Эти угрозы могут быть реализованы в отношении компонентов сбора данных, протоколов взаимодействия, а также подсистемы управления инфраструктурой и подсистемы обработки и хранения данных [1].

При формировании перечня угроз безопасности систем Интернета вещей используют различные источники и публикации Microsoft [2], Kaspersky [3], Cisco [4], Palo Alto [5], содержащие в себе в том числе актуальные сведения об уязвимостях и проблемах, выявленных в данных системах, и позволяющие на основании проанализированных данных делать предположения об актуальности этих угроз.

Исходя из рекомендаций NIST [6], наиболее оптимальной следует считать классификацию данных угроз по направлению воздействия:

- состоянию пользователя;
- конфиденциальности пользователя;
- среде размещения и функционирования;
- модификации или приостановления выполнения задач;
- компрометации IoT-системы и компонентов.

Каждая угроза, входящая в перечисленные группы, может привести к негативным последствиям для пользователей системы или самой системы Интернета вещей и направлена на следующие типы нарушаемых свойств:

- безопасность устройств и компонентов;
- безопасность данных;
- безопасность частной жизни.

На рис. 2 представлены и сгруппированы по объектам воздействия специфические угрозы безопасности, актуальные для систем Интернета вещей.

Угрозы состоянию пользователя системы и его конфиденциальности характеризуются предоставлением со стороны устройств данных, которые потенциально могут негативно повлиять на самого пользователя, его решения, выводы, действия, а также те компоненты системы, через которые пользователь взаимодействует с системой, либо утечкой или модификацией пользовательских данных, в том числе персональных данных, которые собираются, хранятся и используются в системе.

Угрозы среде функционирования характеризуются генерацией, модификацией или уничтожением данных, которые могут негативно повлиять на состояние той физической среды, в которой расположены и функционируют компоненты системы Интернета вещей.


***Рис. 2. Специфические типовые угрозы для систем Интернета вещей***

Данные типы угроз выходят за рамки угроз информационной безопасности в традиционном понимании, но их реализация может привести к нарушениям безопасности информации, нарушениям или прекращению функционирования систем и сетей Интернета вещей. Их следует формулировать и включать в модели угроз для подобных систем, поскольку нельзя не учитывать особенности функционирования и взаимодействия IoT-устройств.

**Литература**


1. *Минзов А. С., Невский А. Ю., Баронов О. Ю.* Информационная безопасность в цифровой экономике // ИТНОУ. 2018. № 3. С. 52—59.

2. IoT security — an overview. Protect your data and devices across the Internet of Things [Электронный ресурс]. URL: https://azure.microsoft.com/ru-ru/overview/internet-of-things-iot/iot-security-cybersecurity (дата обращения: 10.12.2020).

3. Угрозы Интернета вещей и возможные методы защиты [Электронный ресурс]. URL: https://os.kaspersky.ru/2019/03/13/ugrozy-interneta-veshhey-i-vozmozhnye-me/ (дата обращения: 10.12.2020).

4. The Internet of Things: Reduce Security Risks with Automated Policies [Электронный ресурс]. URL: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/security-risks.pdf (дата обращения: 10.12.2020).

5. 2020 Unit 42 IoT Threat Report [Электронный ресурс]. URL: https://start.paloaltonetworks.com/unit-42-iot-threat-report (дата обращения: 10.12.2020).

6. NIST IR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks [Электронный ресурс]. URL: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf (дата обращения: 09.12.2020).


## Cybersecurity threat modeling peculiarities in Internet of Things systems


[1] *P. A. Ivanov,* [1, 2] *I. V. Kapger*

[1] Moscow Power Engineering Institute (MPEI), Moscow, Russia

[2] State National Research Politechnical University of Perm, Perm, Russia



*This article describes cybersecurity threat modeling approach in the Internet of Things systems which takes into account peculiarities of IoT device interaction with each other and system components. This article offers a method of cybersecurity threat modeling based on examination of threats to information resources and system components and risks for users and physical environment.*



*Keywords*: cybersecurity, cybersecurity threats, cybersecurity threat modeling, Internet of Things (IoT).

Bibliography — 6 references. *Received July 9, 2021*

УДК 004
DOI: 10.52190/2073-2600_2021_3_30

# Анализ актуальности и эффективности интегрированных биометрических средств и методов защиты информации в современных системах информационной безопасности

*С. А. Дмитриев*
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

*Проведено изучение основных аспектов, касающихся интегрированных биометрических средств и методов защиты информации в современных системах информационной безопасности. Подзадачами данной работы является изучение актуальности разработки инновационных средств защиты информации, актуальности интеграции биометрических средств и методов защиты информации, эффективности интегрированных биометрических средств и методов защиты информации.*

*Ключевые слова*: биометрические средства, информационная безопасность, информация, информационные технологии, защита информации.

Ввиду развития информационных технологий практически каждая организация или предприятие переводит свои архивы в электронную форму, а также в целом переходит на использование цифровых методов и устройств обработки информации. С помощью информации и информационных технологий передаются конфиденциальные данные и производится их обработка, производятся транзакции на различных предприятиях, выполняются хранение и работа с засекреченной информацией и т. д. Перечень данных процессов можно проводить бесконечно, так как в век информационных технологий практически все процессы, происходящие в жизнедеятельности человека, основываются на применении информационных технологий и информации в частности. Ввиду повсеместного развития информационных и цифровых технологий особенно актуальными задачами становятся обеспечение информационной безопасности и защита информации [1].

Вопросы защиты информации являются достаточно изученными среди многих отечественных и зарубежных исследователей. Несмотря на это, в современном мире все еще существуют колоссальные потенциальные угрозы, связанные с хищением или незаконным доступом к информации. Параллельно с развивающимися технологиями из ИТ-индустрии развиваются и методы несанкционированного доступа со стороны злоумышленников. Организации должны иметь в своем арсенале самые инновационные и эффективные средства обеспечения информационной безопасности. Одними из самых актуальных и, возможно, эффективных средств предотвращения несанкционированного доступа, используемых в системах информационной безопасности, являются биометрические методы защиты информации.

Биометрические методы защиты — это считывание с пользователя уникального биометрического параметра с последующим его сравнением по всей базе уже имеющихся данных. Одним из средств извлечения таких данных являются биометрические считыватели.

## Методы

Основная идея данной работы заключается в попытке обосновать колоссальную актуальность и эффективность использования биометрических средств защиты информации в современных системах информационной безопасности. Применены статистические данные и информация, а также эмпирические и теоретические методы исследования. Для более полного раскрытия темы и получения достоверных данных использованы публикации и материалы отечественных и зарубежных источников. Автор обращается к реальным результатам испытания и оценки эффективности биометрических методов защиты информации. Помимо этого, в целях более детального понимания изучаемой области в оценке эффективности конкретных биометрических методов приведены различные параметры, относительно которых и произведен анализ устойчивости.

**Дмитриев Сергей Александрович**, старший преподаватель кафедры № 203.
E-mail: s-dmi@yandex.ru

*Статья поступила в редакцию 4 июня 2021 г.*

© Дмитриев С. А., 2021

Автор обращается к научным материалам Афанасьевой Д. В., Голеусова Я. А., Масловой М. А., Соколова М. М., Крутохвостова Д. С., Хиценко В. Е. и других. В работах данных авторов раскрываются такие вопросы, как показатели эффективности систем биометрической аутентификации и идентификации, определение рисков информационной безопасности, основные принципы функционирования системы многофакторной биометрической аутентификации, парольная и непрерывная аутентификация по клавиатурному почерку и другие. Таким образом, в используемых материалах раскрываются основные фундаментальные вопросы, касающиеся темы представленного исследования.

## Основные сведения, касающиеся биометрии и биометрической аутентификации

Биометрия — это любая измеримая устойчивая отличительная физическая характеристика или личная черта человека, которая может быть использована для идентификации или проверки заявленной личности этого человека. "Измеримая" означает, что характеристика или признак могут быть преобразованы в цифровой формат. Это позволяет автоматизировать процесс сопоставления в считанные секунды [2].

На рис. 1 представлена обобщенная классификация биометрических средств контроля доступа к информационным ресурсам.

Надежность биометрии определяет, как физическая характеристика или личностная черта изменяются с течением времени. Изменения могут произойти из-за воздействия на человека химических веществ, старения или травм. Высоконадежная биометрия не подвержена значительным изменениям с течением времени, в то время как низкая степень надёжности указывает на биометрию, которая может значительно измениться со временем. Например, шаблоны радужной оболочки, которые изменяются очень мало в течение жизни, более устойчивы, чем голоса.

Отличительная способность — это мера вариаций или различий в биометрической структуре населения в целом. Самая высокая степень отличительности подразумевает уникальный идентификатор, в то время как низкая степень отличительности указывает на биометрический шаблон, часто встречающийся среди населения в целом. Биометрическая аутентификация относится к автоматизированным методам идентификации или проверке личности человека в режиме реального времени на основе физических характеристик или личных качеств.

## Актуальность биометрических методов защиты информации в системах информационной безопасности

Существует огромное количество потенциальных рисков и опасностей, относящихся к области информационной безопасности. Данный фактор вызван повсеместным повышением числа информационных ресурсов, цифровых переводов, коммуникаций и иных продуктов информационной деятельности. Существующий ряд рисков способен привести к колоссальным последствиям в области информационной безопасности [3].

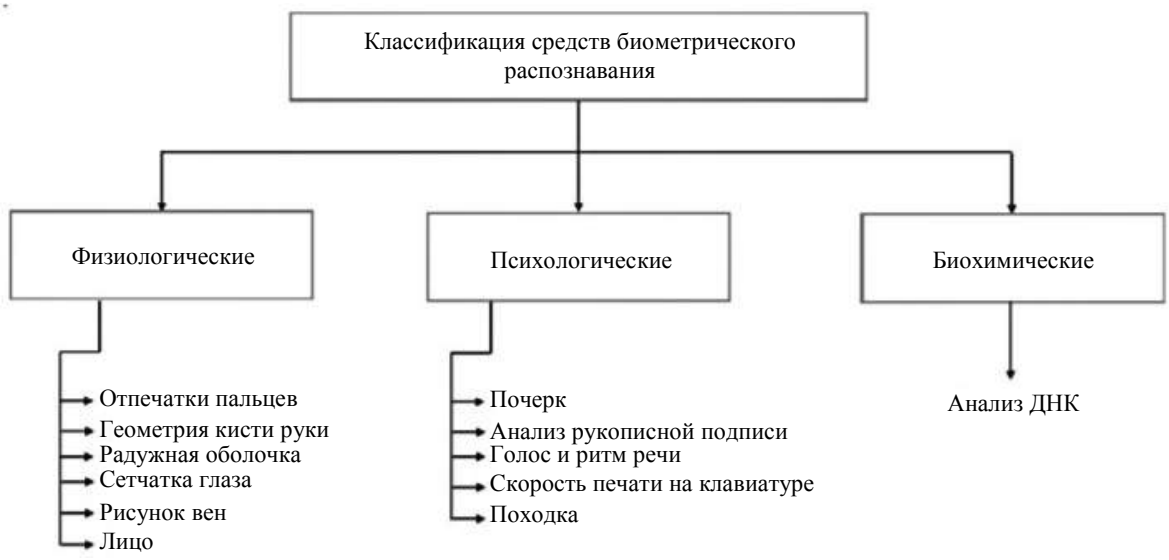



***Рис. 1. Классификация средств биометрии***

Сотрудники информационной безопасности и непосредственно руководители организаций уже признали высокую актуальность и эффективность использования биометрических средств и методов защиты информации. Отмечается высокий рост рынка технологий, связанных с обеспечением защиты информации на основе биометрических методов. На рис. 2 представлена статистическая информация, демонстрирующая непрерывный рост и прогнозируемое значение объема мирового рынка биометрических систем до 2022 г.

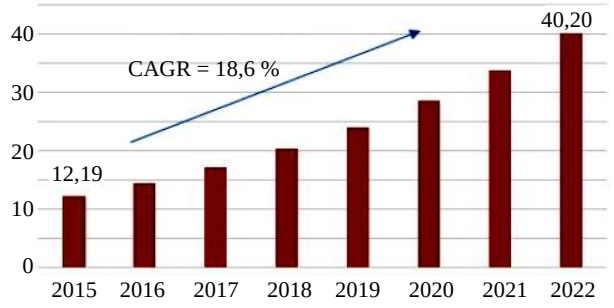



***Рис. 2. Прогноз роста и объем рынка биометрических технологий (в млрд долл.)***

Продолжая изучение темы, необходимо отметить, что существуют достаточно эффективные, но в то же время уязвимые алгоритмы и методы защиты информации. Поэтому современные организации нуждаются в интеграции инновационных средств защиты информации, одним из примеров которых является биометрическая аутентификация.

Актуальность биометрической аутентификации также заключается и в том, что это единственный существующий метод, позволяющий считывать абсолютно уникальные для каждого пользователя биометрические образы. Благодаря этому системы информационной безопасности, использующие в своей работе биометрические методы контроля, отличаются наличием высокого уровня защиты от несанкционированного доступа к информации [4].

## Оценка эффективности методов биометрической идентификации в современных системах информационной безопасности

Результаты оценки эффективности, приведенные в последующих таблицах, будут определять уровень эффективности по отдельным параметрам на основе цветовой палитры: светлый — высокая эффективность; светло-серый — средняя эффективность; темно-серый — низкая эффективность. Перед оценкой эффективности работы методов биометрической аутентификации пользователей определим параметры оценки. Главными для оценки любой биометрической системы являются два параметра:

- FAR (False Acceptance Rate) — коэффициент ложного пропуска, т. е. процент возникновения ситуаций, когда система разрешает доступ пользователю, незарегистрированному в системе;
- FRR (False Rejection Rate) — коэффициент ложного отказа, т. е. отказ в доступе настоящему пользователю системы.

Обе характеристики получают расчетным путем на основе методов математической статистики. Для самых популярных методов биометрической идентификации средние значения FAR и FRR приведены в табл. 1.

Таблица 1

**Значения FAR и FRR методов биометрической идентификации**

| Биометрический метод | FAR, % | FRR, % |
|---|---|---|
| Отпечаток пальца | 0,001 | 0,6 |
| Распознавание лица 2D | 0,1 | 2,5 |
| Распознавание лица 3D | 0,0005 | 0,1 |
| Радужная оболочка глаза | 0,00001 | 0,016 |
| Сетчатка глаза | 0,0001 | 0,4 |

Далее будет проведено сравнение биометрических методов по устойчивости к фальсификации данных. Фальсификация биометрических данных — это в любом случае достаточно сложный процесс, зачастую требующий специальной подготовки и технического сопровождения. В табл. 2 приведены результаты исследований, отображающие возможность фальсификации биометрических параметров [5].

Таблица 2

**Сравнение биометрических методов по устойчивости к фальсификации**

| Биометрический метод | Фальсификация |
|---|---|
| Отпечаток пальца | Возможна |
| Распознавание лица 2D | Проблематична |
| Распознавание лица 3D | Безуспешна |
| Радужная оболочка глаза | Невозможна |
| Сетчатка глаза | Невозможна |

Произведем анализ биометрических методов относительно устойчивости к внешним факторам. В табл. 3 представлены результаты чувствительности методов биометрической аутентификации к параметрам окружающей среды.

Таблица 3

**Сравнение биометрик по чувствительности к внешним факторам**

| Биометрический метод | Чувствительность к влиянию внешних факторов |
|---|---|
| Отпечаток пальца | Средняя |
| Распознавание лица 2D | Низкая |
| Распознавание лица 3D | Низкая |
| Радужная оболочка глаза | Низкая |
| Сетчатка глаза | Средняя |

Как видно из представленных в табл. 1—3 данных, средства биометрической аутентификации пользователя в техническом плане являются достаточно эффективным и успешно функционирующим инструментом. В большинстве метрик, по которым была произведена оценка эффективности, биометрические методы аутентификации пользователя показали высокие результаты в оценке эффективности их использования.

Безусловно, выбор метода биометрической аутентификации для системы контроля доступа в первую очередь зависит от предъявляемых к ней требований. Тем не менее сравнение биометрических методов по совокупности факторов наглядно демонстрирует их преимущества в целом [6].

## Заключение

Существующие средства и методы защиты информации становятся наиболее подверженными удачным взломам и несанкционированному доступу, в результате чего актуализируется роль разработки и интеграции инновационных средств обеспечения защищенности информации. Исходя из этого, наиболее актуальными становятся задачи, решения которых позволяют повысить эффективность и рациональность работы систем информационной безопасности, одним из которых и является разработка и повсеместная интеграция биометрических методов защиты информации [7].

Главной целью представленной работы являлось изучение. Гипотеза исследования основных аспектов, касающихся биометрических средств и методов защиты информации в системах информационной безопасности, заключалась в том, что биометрические методы защиты информации являются наиболее эффективным инструментом, способным обеспечить высокий уровень защиты информации в системах информационной безопасности. Автором исследованы аспекты, посредством которых была подтверждена заявленная гипотеза.

Необходимо отметить, что современные организации, желающие обеспечить высокий уровень надежности и эффективности систем информационной безопасности, должны непременно обратить внимание на биометрические методы защиты информации. Изученные в данной статье методы защиты информации не только доказали свою эффективность, но также имеют и колоссальный потенциал, который необходимо раскрывать в дальнейших исследованиях и разработках.

**Литература**


1. *Афанасьева Д. В.* Применение искусственного интеллекта в обеспечении безопасности данных // Изв. ТулГУ. Технические науки. 2020. № 2. С. 151—154.
2. *Голеусов Я. А.* О показателях эффективности систем биометрической аутентификации и идентификации // Актуальные проблемы авиации и космонавтики. 2016. Т. 1. № 12. С. 752—754.
3. *Маслова М. А.* Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. 2019. Т. 4. № 1. С. 31—37.
4. *Спеваков А. Г.* Методы идентификации личности человека по морфологическим признакам // Сб. мат. IX международной конференции «Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации. Распознавание – 2010». Курск, 18—20 мая 2010 г. С. 53—54.
5. *Голеусов Я. А., Соколов М. М.* Об основных принципах функционирования системы многофакторной биометрической аутентификации по динамике нажатия клавиш // Решетневские чтения. 2015. Т. 2. С. 277—279.
6. *Крутохвостов Д. С., Хиценко В. Е.* Парольная и непрерывная аутентификация по клавиатурному почерку средствами математической статистики // Вопросы кибербезопасности. 2017. № 5 (24). С. 91—99.
7. *Чеснокова А. А., Калуцкий И.В., Спеваков А. Г.* Электронный документооборот: безопасность на этапах внедрения и эксплуатации // Известия Юго-Западного государственного университета. Серия: управление, вычислительная техника, информатика. Медицинское приборостроение. 2017. Т. 7. № 4 (25). С. 13—23.


# Analysis of the relevance and effectiveness of integrated biometric means and methods of information protection in modern information security systems


*S. A. Dmitriev*

Moscow Aviation Institute (National Research University), Moscow, Russia



*The main purpose of the presented work is to study the main aspects related to integrated biometric means and methods of information protection in modern information security systems. The subtasks of this work: studying the relevance of the development of innovative means of protecting information; study of the relevance of the integration of biometric means and methods of information protection; study of the effectiveness of integrated biometric means and information security methods.*



*Keywords:* biometric tools, information security, information, information technology, information security.

Bibliography — 7 references. *Received June 4, 2021*

УДК 004
DOI: 10.52190/2073-2600_2021_3_34

# Обоснование актуальности обеспечения информационной безопасности сетей Интернета вещей посредством разработки методов машинного обучения

*Д. С. Карнута*
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

*Проведено изучение методов машинного обучения применительно к вопросу информационной безопасности сетей Интернета вещей. Изучены актуальность разработки и интеграции систем информационной безопасности для данных сетей в целом, актуальность разработки систем информационной безопасности на основе методов машинного обучения. Приведен обзор возможной разработки и интеграции отдельных методов машинного обучения. Гипотеза представленного исследования заключается в том, что методы машинного обучения представляют из себя колоссальную базу, способную обеспечить целостность и сохранность информационных ресурсов, а также обеспечить в целом высокий уровень системы информационной безопасности в сетях Интернета вещей. Приводится информация, подтверждающая заявленную гипотезу, на основе которой строятся оригинальные выводы.*

*Ключевые слова*: Интернет вещей, информационная безопасность, машинное обучение, информация, вычислительная техника.

Интернет вещей (IoT) объединяет миллиарды смарт-устройств, которые могут взаимодействовать друг с другом с минимальным вмешательством человека. Это одна из самых быстроразвивающихся областей в истории вычислительной техники. К концу 2020 г. она оценивалась в 50 миллиардов устройств. С одной стороны, технологии IoT играют решающую роль в усовершенствовании многих смарт-приложений, способных улучшить качество жизни. С другой стороны, сквозная природа систем IoT и компонентов, участвующих в развертывании таких систем, привела к новым проблемам безопасности. Реализация мер безопасности, таких, как шифрование, аутентификация, контроль доступа, сетевая безопасность и безопасность приложений, для устройств IoT и их уязвимых мест неэффективна. Поэтому существующие методы обеспечения безопасности должны быть улучшены для эффективной защиты экосистемы IoT [1].

Машинное обучение и глубокое обучение (ML/DL) значительно продвинулись и машинный интеллект перешел от лабораторного исследования к практическому механизму в нескольких важных приложениях. Возможность интеллектуального мониторинга IoT-устройств обеспечивает решение задач безопасности для новых атак или атак нулевого дня. ML/DL являются мощными методами исследования данных для изучения "нормального" и "ненормального" поведения в соответствии с тем, как компоненты и устройства IoT работают в среде IoT. Следовательно, методы ML/DL важны для улучшения безопасности систем IoT от упрощения безопасного обмена данными между устройствами до построения интеллектуальных защищенных систем.

## Методы

Цель работы — рассмотреть угрозы безопасности IoT-систем и провести анализ методов машинного обучения для решения задач из данного сегмента посредством применения статистических данных и информации, а также эмпирических и теоретических методов исследования. Для более полного раскрытия темы и получения достоверных данных использованы публикации и материалы отечественных и зарубежных источников. Автор использует эмпирические, теоретические и статистические методы исследования.

Изучены научные материалы Цветковой О. Л., Крепера А. И., Полегенько А. М., Афанасьевой Д. В., Тершукова Д. А., Drone K. K., Maslova M. A. и других. Каждый из указанных научных материалов раскрывает отдельные аспекты, касающиеся темы представленного исследования. В использу-

**Карнута Дмитрий Сергеевич**, начальник учебной части — заместитель начальника кафедры УВП МО РФ ВУЦ.
E-mail: dima-karnuta@mail.ru

*Статья поступила в редакцию 25 мая 2021 г.*

© Карнута Д. С., 2021

емых научных материалах раскрываются вопросы применения теории искусственных нейронных сетей в решении задач обеспечения информационной безопасности, особенностей защиты информации в Интернете вещей, проблем безопасности Интернета вещей и т. д. [1—5].

## Обоснование актуальности разработки способа повышения безопасности IoT-систем

Прогресс в информационных технологиях, таких, как Интернет вещей, значительно расширил традиционное восприятие окружающей среды. Технологии IoT могут способствовать модернизации, улучшающей качество жизни. С одной стороны, технологии IoT играют решающую роль в улучшении реальных смарт-приложений, таких, как смарт-здравоохранение, умные дома, смарт-транспортные средства и смарт-образование. С другой стороны, сквозной и крупномасштабный характер систем IoT с различными компонентами, участвующими в развертывании таких систем, привел к возникновению новых проблем безопасности.

Системы IoT являются сложными и содержат интегративные механизмы. Следовательно, поддержание требований безопасности на широкомасштабной поверхности атаки системы IoT является сложной задачей. Решения должны включать в себя комплексные соображения для удовлетворения требований безопасности. Однако устройства IoT в основном работают в автоматической среде. Следовательно, злоумышленник может физически получить доступ к этим устройствам. Устройства IoT обычно подключаются по беспроводным сетям, где злоумышленник может получить доступ к частной информации из канала связи путем прослушивания [2].

Устройства IoT не могут поддерживать сложные структуры безопасности из-за их ограниченных вычислительных и энергетических ресурсов. Сложные структуры безопасности IoT обусловлены не только ограниченными вычислительными, коммуникационными и энергетическими ресурсами, но и надежным взаимодействием с физической областью, в частности поведением физической среды в непредсказуемых обстоятельствах, поскольку системы IoT также являются частью киберфизической системы. Системы IoT должны постоянно адаптироваться и выживать точным и предсказуемым образом, а безопасность должна быть ключевым приоритетом, особенно в условиях, когда могут возникнуть серьезные последствия, такие, как в системах здравоохранения. Более того, новые поверхности атаки представлены средой IoT. Такие поверхности атаки вызваны взаимозависимыми и взаимосвязанными средами IoT. Следовательно, риски угрозы безопасности в IoT-системах выше, чем в других вычислительных системах, и традиционное решение может оказаться неэффективным для таких систем.

Важным следствием широкого применения IoT является то, что развертывание IoT становится взаимосвязанной задачей. Например, системы IoT должны одновременно учитывать эффективность использования энергии, безопасность, методы анализа больших данных IoT и взаимодействие с программными приложениями на этапе развертывания. Эта интеграция предоставляет исследователям из междисциплинарных областей новую возможность изучать текущие проблемы в системах IoT с разных точек зрения. Однако эта интеграция также создает новые проблемы безопасности из-за характера распространения устройств IoT, которые обеспечивают большую и уязвимую поверхность. Эта характеристика IoT-устройств связана со многими проблемами безопасности. Более того, платформа IoT генерирует большой объем ценных данных. Если эти данные не передаются и не анализируются надежно, это может привести к серьезному нарушению конфиденциальности.

Системы IoT доступны во всем мире, состоят в основном из ограниченных ресурсов и построены на каналах с потерями. Следовательно, для обеспечения эффективных методов безопасности IoT должны быть реализованы важные модификации существующих концепций безопасности для информационных и беспроводных сетей. Применение существующих защитных механизмов, таких, как шифрование, аутентификация, контроль доступа, сетевая безопасность и безопасность приложений, является сложным и недостаточным для комплексных систем с множеством подключенных устройств, где каждая часть системы имеет присущие ей уязвимости.

## Характеристики безопасности IoT-систем

IoT интегрирует Интернет с физическим миром, чтобы обеспечить разумное взаимодействие между физическим миром и его окружением. Как правило, устройства IoT работают в разных средах для достижения разных целей. Тем не менее их работа должна соответствовать требованию комплексной безопасности в кибер и физических состояниях. Системы IoT являются комплексными, следовательно, поддержание требований безопас-

ности при широкомасштабной поверхности атаки системы IoT является сложной задачей. Чтобы удовлетворить данное требование, решение должно иметь комплексные соображения. Однако устройства IoT в основном работают в автоматической среде. Следовательно, злоумышленник может физически получить доступ к этим устройствам. Устройства IoT обычно подключаются по беспроводным сетям, где злоумышленник может раскрыть личную информацию из канала связи путем прослушивания. Устройства IoT не могут поддерживать сложные структуры безопасности из-за их ограниченных вычислительных и энергетических ресурсов [3].

Учитывая, что основной целью системы IoT является предоставление доступа кем угодно, где угодно и когда угодно, векторы атаки также становятся доступными для атакующих. Следовательно, потенциальные угрозы становятся более вероятными. Угроза — это акт, который может использовать слабые места системы безопасности и оказывать на нее негативное влияние. Многочисленные угрозы, такие, как пассивные атаки (например, подслушивание), и активные угрозы (например, спуфинг, Sybil, man-in-the-middle), могут повлиять на систему IoT.

Перечисленные далее основные характеристики безопасности следует учитывать при разработке эффективных методов безопасности IoT.

- *Конфиденциальность*. Конфиденциальность является важной характеристикой безопасности систем IoT. Устройства IoT могут хранить и передавать конфиденциальную информацию, которая не должна раскрываться посторонними лицами.
- *Целостность*. Данные от устройств IoT обычно передаются по беспроводной связи и могут быть изменены только уполномоченными лицами. Таким образом, функции целостности, имеют основополагающее значение для обеспечения эффективного механизма проверки для обнаружения любых изменений во время связи по небезопасной беспроводной сети.
- *Аутентификация*. Личность объектов должна быть полностью установлена до выполнения любого другого процесса. Однако из-за характера систем IoT требования к аутентификации отличаются от системы к системе. Следовательно, система IoT требует эффективной аутентификации, которая может сбалансировать системные ограничения и обеспечить надежные механизмы безопасности.
- *Авторизация*. Авторизация предоставляет пользователям право доступа к системе IoT, так же, как и к физическим датчикам. Основная проблема авторизации в средах IoT заключается в том, как успешно предоставить доступ в среде, где не только люди, но и физические датчики (вещи) должны иметь право взаимодействовать с системой IoT.
- *Доступность*. Услуги, предоставляемые системами IoT, всегда должны быть доступны уполномоченным лицам. Доступность является фундаментальной особенностью успешного развертывания систем IoT.
- *Безотказность*. Свойство безотказности предназначено для предоставления журналов доступа, которые служат доказательством в ситуациях, когда пользователи или объекты не могут отказаться от действия [4].

## Методы машинного обучения применительно к IoT-системам

Алгоритмы обучения широко применяются во многих реальных приложениях из-за их уникальной природы решения проблем. Такие алгоритмы способны прогрессировать автоматически благодаря получению опыта. Алгоритмы обучения широко применяют на практике. Текущее развитие алгоритмов обучения обусловлено разработкой новых алгоритмов и доступностью больших данных в дополнение к появлению алгоритмов с низкими затратами на вычисления. ML и DL значительно продвинулись, а машинный интеллект перешел от лабораторного исследования к практическому механизму в нескольких важных приложениях. Несмотря на то что DL является подмножеством ML, ML относится к традиционным методам ML, которые требуют инженерных функций, в то время как методы DL относятся к последним достижениям в методах обучения, которые используют несколько уровней нелинейной обработки для абстрагирования и преобразования дискриминационных или порождающих признаков для анализа паттернов.

Как правило, алгоритмы обучения направлены на повышение производительности при выполнении задачи с помощью тренировки и обучения на основе опыта. Например, при обучении обнаружению вторжений задача состоит в том, чтобы классифицировать поведение системы как нормальное или ненормальное. Улучшение производительности может быть достигнуто за счет повышения точности классификации, а опыт, полученный из алгоритмов, представляет собой совокупность нормального поведения системы. Алгоритмы обучения подразделяют на три основные категории: контролируемое, неконтролируемое и усиленное обучение (RL).

Рассматриваемые методы обучения формируют свою классификацию или модель прогнозирования на основе изученного отображения и наблюдения за входными параметрами. Другими словами, эти методы фиксируют отношения между входными параметрами (функциями) и требуемым выходом. Следовательно, на начальном этапе контролируемого обучения необходимы обучающие примеры для обучения алгоритмов, которые затем используются для прогнозирования или классификации новых входных данных. Произошедшее огромное продвижение в контролируемом обучении вовлекает глубокие сети. Эти сети можно рассматривать как многослойные сети с пороговыми единицами, каждая из которых рассчитывает функцию своего входа [5].

## Обзор классических методов машинного обучения для безопасности IoT-систем

Рассмотрим общие методы машинного обучения для безопасности IoT-систем, а также их преимущества, недостатки и применение в безопасности IoT.

*Методы деревьев принятия решений (DT)*. Методы на основе DT в основном классифицируют путем сортировки образцов в соответствии с их значениями. Каждая вершина (узел) в дереве представляет элемент, а каждое ребро (ветвь) обозначает значение, которое может иметь вершина в образце для классификации. Выборки классифицируются, начиная с вершины происхождения, по значениям их признаков. Особенностью, которая оптимально разбивает обучающие выборки, считается исходная вершина дерева. Для определения оптимальной функции, которая наилучшим образом разделяет обучающие выборки, используют несколько мер, включая прирост информации и индекс Джини.

Большинство подходов, основанных на DT, состоит из двух основных процессов: построение (индукция) и классификация (вывод). В процессе построения DT обычно создается с помощью дерева с незанятыми узлами и ветвями. Впоследствии признак, который лучше всего расщепляет обучающие выборки, считается исходной вершиной дерева. Эта функция выбирается с помощью различных мер, таких, как прирост информации. Смысл состоит в том, чтобы назначить корневые узлы признаков, которые максимально уменьшают область пересечения между классами в обучающем наборе, улучшая таким образом способность различения классификатора. Та же процедура применяется к каждому подчиненному дереву, пока не будут получены листья и установлены соответствующие классы. В процессе классификации после построения дерева новые выборки с набором признаков и неизвестным классом классифицируют, начиная с корневых узлов построенного дерева (т. е. дерева, построенного в процессе обучения) и продолжая путь, соответствующий изученным значениям признаков во внутренних узлах дерева. Эта процедура продолжается, пока лист не найден. В итоге соответствующие метки (т. е. предсказанные классы) новых образцов бывают получены.

Основные недостатки методов, основанных на DT, сводятся к следующему. Во-первых, они требуют много места из-за особенностей конструкции. Во-вторых, понимание методов на основе DT является легким только, в том случае, если задействовано несколько DT. Однако в некоторых приложениях используется массивная конструкция деревьев и нескольких узлов принятия решений. В этих приложениях сложность вычислений высока, а базовая модель для классификации выборок является сложной.

DT используется в качестве основного классификатора для совместной работы с другими классификаторами ML в приложениях безопасности, таких, как обнаружение вторжений. Например, в исследовании предлагалось использовать систему системных вызовов на основе туманных вычислений для защиты устройств IoT. Исследование использовало DT для анализа сетевого трафика, чтобы обнаружить подозрительные источники трафика и, следовательно, выяснить поведение DDoS.

*Машины опорных векторов (SVM)*. SVM используют для классификации путем создания гиперплоскости расщепления в атрибутах данных между двумя или более классами так, чтобы расстояние между гиперплоскостью и наиболее смежными точками выборки каждого класса было максимальным. SVM отличаются возможностью обобщения и особенно подходят для наборов данных с большим количеством атрибутов признаков, но небольшим количеством точек выборки. Теоретически SVM были созданы из статистического обучения.

Первоначально SVM были созданы для категоризации линейно делимых классов в двумерную плоскость, содержащую линейно разделяемые точки данных разных классов (например, нормальные или ненормальные). SVM должны создавать превосходную гиперплоскость, которая обеспечивает максимальный запас, увеличивая расстояние между гиперплоскостью и наиболее

смежными точками выборки каждого класса. Преимуществами SVM являются их масштабируемость, возможность выполнять обнаружение вторжений в режиме реального времени и динамическое обновление шаблонов обучения.

SVM широко используют в различных приложениях безопасности, таких, как обнаружение вторжений. Они эффективны с точки зрения использования памяти, поскольку создают гиперплоскость для разделения точек данных с временной сложностью, равной O(N^2), где N относится к числу образцов. В отношении среды IoT разработана система обнаружения вредоносных программ Android для ее защиты и применен линейный SVM к их системе. Тем не менее дополнительные исследования необходимы для изучения производительности SVM с увеличенными наборами данных и наборами данных, созданными в различных средах и сценариях атак [2].

*Случайный лес (RF).* RF являются контролируемыми алгоритмами обучения. В RF несколько DT построено и объединено, чтобы получить точную и надежную модель прогнозирования для улучшения общих результатов. Следовательно, RF состоит из множества деревьев, которые построены случайным образом и обучены голосовать за класс. Класс с наибольшим количеством голосов выбирается в качестве окончательного результата классификации.

Несмотря на то что RF-классификатор построен в основном с использованием DT, эти алгоритмы классификации существенно различаются. Во-первых, DT обычно формулируют набор правил, когда обучающий набор подается в сеть, и этот набор правил впоследствии используется для классификации нового ввода. RF использует DT для построения подмножеств правил для голосования по классу. Таким образом, результат классификации является средним из результатов и RF устойчива к перестройке. Кроме того, RF обходит выбор функции и требует только нескольких входных параметров. Тем не менее использование RF может быть нецелесообразным в конкретных приложениях реального времени, в которых требуемый набор обучающих данных велик, потому что RF требует построения нескольких DT.

## Заключение

Рассмотрен ряд основных моментов, раскрывающих актуальность вопроса защиты информации в сетях Интернета вещей, а также актуальность интеграции методов машинного обучения для их решения. Освещены вопросы: актуальности разработки способа повышения безопасности IoT-систем, характеристики безопасности IoT-систем, методы машинного обучения применительно к IoT-системам.

Таким образом, доказана представленная изначально гипотеза, связанная с высокой актуальностью и эффективностью разработки методов машинного обучения для реализации мер информационной безопасности в сетях Интернета вещей. Исходя из всей представленной информации можно отметить, что, с одной стороны, технологии IoT играют решающую роль в улучшении многих смарт-приложений, способных улучшить качество жизни. С другой стороны, сквозная природа систем IoT и компонентов, участвующих в развертывании таких систем, привела к новым проблемам безопасности, которые требуют незамедлительного решения на основе разработки инновационных методов защиты информации.

**Литература**


1. *Цветкова О. Л., Крепер А. И.* О применении теории искусственных нейронных сетей в решении задач обеспечения информационной безопасности // Символ науки. 2017. Т. 2. № 4. С. 105—107.
2. *Полегенько А. М.* Особенности защиты информации в Интернете вещей // International J. Open Information Technologies. 2018. Т. 6. № 10. Р. 41—45.
3. *Афанасьева Д. В.* Применение искусственного интеллекта в обеспечении безопасности данных // Изв. ТулГУ. Технические науки. 2020. № 2. С. 151—154.
4. Тершуков Д. А. Анализ современных угроз информационной безопасности // НБИ Технологии. 2018. Т. 12. № 3. С. 6—12.
5. *Дрон К. К.* О перспективах совместного использования методов квантовой и классической криптографии // Вестник ХГУ им. Н. Ф. Катанова. 2018. № 24. С. 8—11.

# Substantiation of the relevance of ensuring the information security of the Internet of things networks through the development of machine learning methods

*D. S. Karnuta*
Moscow Aviation Institute (National Research University), Moscow, Russia

*The studied of machine learning methods in relation to the issue of information security of networks of the Internet of Things networks. The relevance of the development and integration of information security systems for these networks in general, the relevance of the development of information security systems based on machine learning methods have been studied. An overview of the possible development and integration of individual machine learning methods is given. The hypothesis of the presented study is that machine learning methods are a colossal base capable of ensuring the integrity and safety of information resources, as well as providing a generally high level of information security in the Internet of Things networks. Information is provided that confirms the stated hypothesis, on the basis of which the original conclusions are based.*

*Keywords*: Internet of Things, information security, machine learning, information, computing.

Bibliography — 6 references. *Received May 25, 2021*

## ЭЛЕКТРОННАЯ ПОДПИСЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 003.26
DOI: 10.52190/2073-2600_2021_3_40

# Постквантовый алгоритм цифровой подписи на коммутативной алгебре

*А. А. Молдовян,* д-р техн. наук
Санкт-Петербургский федеральный исследовательский центр РАН, Санкт-Петербург, Россия

*Предложен новый способ построения постквантовых схем цифровой подписи на коммутативных алгебрах, мультипликативная группа которых обладает многомерной цикличностью. В основу способа положен метод удвоения проверочного уравнения. Новым является комбинирование векторного и скалярного умножения при формировании открытого ключа. Вычислительно трудная задача, используемая в предложенном способе, отнесена к типу скрытой задачи дискретного логарифмирования.*

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

Некоммутативные конечные ассоциативные алгебры (КАА) представляют интерес в качестве алгебраических носителей алгоритмов коммутативного шифрования [1], постквантовых протоколов открытого согласования ключа [2, 3] и электронной цифровой подписи (ЭЦП) [4, 5], стойкость которых связана с вычислительной трудностью так называемой скрытой задачи дискретного логарифмирования (СЗДЛ). Класс задач по вычислению дискретного логарифма в конечной циклической группе при неявно заданных параметрах классической задачи дискретного логарифмирования относится к СЗДЛ [6, 7]. При построении двухключевых криптосхем на основе СЗДЛ открытый ключ вычисляется в зависимости от элементов некоторой скрытой коммутативной группы, в которой выполняется операция возведения в степень, вносящая основной вклад в стойкость криптосхемы. Способность таких криптосхем противостоять квантовым атакам (атакам с использованием квантовых компьютеров) определяется тем, что указанная коммутативная группа маскируется. Для получения возможности обеспечения хорошей маскировки алгебраический носитель криптосхемы должен содержать достаточно большое число изоморфных коммутативных групп и предоставлять возможность задания соответствующего механизма маскирования. Наиболее подходящим алгебраическим носителем до последнего времени представлялись некоммутативные КАА, заданные над простым конечным полем $GF(p)$ с характеристикой, равной простому числу $p$ достаточно большого размера [8, 9].

В работе [10] предложен способ задания СЗДЛ в коммутативных КАА, содержащих мультипликативную группу, обладающую многомерной цикличностью. К группам последнего типа относятся конечные коммутативные группы с двумя или более порождающими элементами, обладающими одним и тем же значением порядка. Одинаковость порядка порождаемых элементов является признаком, выделяющим группы с многомерной цикличностью [11]. Работа [10] показывает принципиальную возможность использования коммутативных КАА в качестве алгебраического носителя схем электронной цифровой подписи (ЭЦП). На настоящий момент алгоритм ЭЦП [10] представляется некоторым исключением из общего правила. Однако не дается ответ на вопрос о существовании других способов построения постквантовых схем ЭЦП на коммутативных КАА. В связи с этим представляет значительный интерес задача разработки новых способов построения схем ЭЦП, основанных на СЗДЛ, при использовании коммутативных КАА. Наличие новых способов будет означать формирование нового направления в области постквантовых схем ЭЦП, основанных на СЗДЛ, которое отличается использованием коммутативных КАА.

В данной работе проведен анализ схемы ЭЦП [10] и предложен новый способ построения постквантовых схем ЭЦП на коммутативных КАА.

**Молдовян Александр Андреевич**, профессор.
E-mail: maa1305@yandex.ru

*Статья поступила в редакцию 1 августа 2021 г.*

© Молдовян А. А., 2021

### Анализ известной схемы ЭЦП

В качестве алгебраического носителя схемы ЭЦП [10] используется коммутативная четырехмерная КАА, заданная над простым конечным полем $GF(p)$ с характеристикой в виде простого числа $p = 2q + 1$, где $q$ — 256-битное простое число. При этом легко предложить алгоритм нахождения векторов порядка $q$, генерирующих различные циклические группы. В частности, в работе [10] использована КНАА, операция векторного умножения в которой задана по таблице.

**Задание умножения в четырехмерной коммутативной КАА ($\lambda = 4$)**

| • | $\mathbf{e}_0$ | $\mathbf{e}_1$ | $\mathbf{e}_2$ | $\mathbf{e}_3$ |
|---|---|---|---|---|
| $\mathbf{e}_0$ | $\lambda\mathbf{e}_2$ | $\mathbf{e}_3$ | $\mathbf{e}_0$ | $\lambda\mathbf{e}_1$ |
| $\mathbf{e}_1$ | $\mathbf{e}_3$ | $\mathbf{e}_2$ | $\mathbf{e}_1$ | $\mathbf{e}_0$ |
| $\mathbf{e}_2$ | $\mathbf{e}_0$ | $\mathbf{e}_1$ | $\mathbf{e}_2$ | $\mathbf{e}_3$ |
| $\mathbf{e}_3$ | $\lambda\mathbf{e}_1$ | $\mathbf{e}_0$ | $\mathbf{e}_3$ | $\lambda\mathbf{e}_2$ |

В коммутативной КАА, заданной по таблице, единицей является вектор (0, 0, 1, 0). Мультипликативная группа этой алгебры обладает четырехмерной (двухмерной) цикличностью при значении $\lambda$, равном квадратичному вычету (невычету) в поле $GF(p)$. В случае формирования группы с двухмерной цикличностью ее базис включает два вектора, имеющих порядок $p^2 - 1$, при значении порядка группы $(p^2 - 1)^2$. Для построения схемы ЭЦП, основанной на СЗДЛ, используется значение $\lambda = 4$. Последнее значение является квадратичным вычетом и определяет четырехмерную цикличность мультипликативной группы. Базис последней включает четыре вектора, каждый из которых имеет порядок $p - 1$. Порядок мультипликативной группы равен $(p - 1)^4$.

Открытый ключ генерируется следующим образом.

- Сгенерировать случайные векторы **G**, **Q**, **U** и **D**, порядок каждого из которых равен одному и тому же простому числу $q$.
- Сгенерировать случайное натуральное число $x < q$ и вычислить векторы $\mathbf{Y}_1 = \mathbf{G}^x\mathbf{U}$ и $\mathbf{Y}_2 = \mathbf{Q}^x\mathbf{U}$.
- Вычислить векторы $\mathbf{Z}_1 = \mathbf{GD}$ и $\mathbf{Z}_2 = \mathbf{QD}$.

Открытым ключом являются две пары векторов: ($\mathbf{Y}_1$, $\mathbf{Z}_1$) и ($\mathbf{Y}_2$, $\mathbf{Z}_2$). Личным секретным ключом владельца этого открытого ключа является набор значений $x$, **G**, **Q**, **U** и **D**, знание которых требуется для вычисления ЭЦП. Вероятность того, что векторы $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ и $\mathbf{Z}_2$ образуют базис примарной группы порядка $q^4$, практически равна 1. Действительно, эти четыре вектора являются случайными, поскольку зависят от случайных векторов **G**, **Q**, **U** и **D**. Вероятность того, что произведения всевозможных степеней векторов $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ и $\mathbf{Z}_2$ образуют примарную подгруппу порядка $q^3$ или $q^2$, пренебрежимо мала и имеет значение $\approx q^{-1}$ (если $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ независимы и образуют примарную группу порядка $q^3$, то вероятность того, что случайный вектор $\mathbf{Z}_2$ содержится в этой примарной группе, равна отношению ее порядка к числу всех векторов, содержащихся в мультипликативной группе рассматриваемой четырехмерной алгебры и имеющих порядок $q$; учет случая, когда $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$ образуют примарную группу порядка $q^2$, вносит небольшую поправку в значение $q^{-1}$).

Пусть дан электронный документ $M$, к которому надо сформировать цифровую подпись владельца открытого ключа ($\mathbf{Y}_1$, $\mathbf{Z}_1$) и ($\mathbf{Y}_2$, $\mathbf{Z}_2$). Для этого выполняется следующая процедура, в которой используется некоторая заранее оговоренная стойкая 256-битная хэш-функция $f_h$ (алгоритм ее вычисления является частью рассматриваемой схемы ЭЦП).

Схема ЭЦП:

- Сгенерировать три случайных натуральных числа $k < q$, $t < q$ и $u < q$.
- Вычислить два вектора-фиксатора $\mathbf{V}_1$ и $\mathbf{V}_2$ по следующим формулам:

$$\mathbf{V}_1 = \mathbf{G}^k\mathbf{D}^t\mathbf{U}^u \text{ и } \mathbf{V}_2 = \mathbf{Q}^k\mathbf{D}^t\mathbf{U}^u.$$

- Вычислить значение $e = f_h(M, \mathbf{V}_1, \mathbf{V}_2)$ (первый элемент ЭЦП).
- Вычислить значение $s = k - ex \bmod q$ (второй элемент ЭЦП).
- Вычислить вектор $\mathbf{S} = \mathbf{D}^{t-e}\mathbf{U}^{u-s}$ (третий элемент ЭЦП).

На выходе этого алгоритма получаем цифровую подпись ($e$, $s$, **S**). Основной вклад в вычислительную сложность алгоритма $W$ вносят операции возведения в степень в рассматриваемой четырехмерной алгебре, т. е. можно принять оценку $W = 8$ операций экспоненцирования.

Алгоритм проверки тройки значений ($e$, $s$, **S**) как подлинной подписи к документу $M$ включает следующие шаги.

- Используя открытый ключ, а именно две пары векторов ($\mathbf{Y}_1$, $\mathbf{Z}_1$) и ($\mathbf{Y}_2$, $\mathbf{Z}_2$), вычислить векторы $\tilde{\mathbf{V}}_1 = \mathbf{Y}_1^e \circ \mathbf{S} \circ \mathbf{Z}_1^s$ и $\tilde{\mathbf{V}}_2 = \mathbf{Y}_2^e \circ \mathbf{S} \circ \mathbf{Z}_2^s$.
- Присоединив к документу векторы $\tilde{\mathbf{V}}_1$ и $\tilde{\mathbf{V}}_2$, вычислить значение хэш-функции $\tilde{e} = f_h\left(M, \tilde{\mathbf{V}}_1, \tilde{\mathbf{V}}_2\right)$.
- Проверить выполнимость равенства $\tilde{e} = e$. Если оно справедливо, то ЭЦП ($e$, $s$, **S**) считается подлинной. Если $\tilde{e} \neq e$, то подпись ($e$, $s$, **S**) отклоняется.

Вычислительная сложность алгоритма проверки подлинности ЭЦП равна $W = 4$ операций экспоненцирования.

Для схемы ЭЦП [10] имеется следующая возможность сведения ее стойкости к решению обычной задачи дискретного логарифмирования. Последняя задается по элементам открытого ключа в виде следующего уравнения:

$$\mathbf{Y}_1\mathbf{Y}_2^{-1} = \mathbf{G}^x\mathbf{Q}^{-x} = (\mathbf{G}\mathbf{Q}^{-1})^x = (\mathbf{Z}_1\mathbf{Z}_2^{-1})^x,$$

записанного в конечной циклической группе, генерируемой вектором $\mathbf{G}\mathbf{Q}^{-1} = \mathbf{Z}_1\mathbf{Z}_2^{-1}$.

### Предлагаемый способ построения схемы ЭЦП

Для устранения выявленного недостатка в способе построения схемы ЭЦП [10], использующем метод удвоения проверочного уравнения [12, 13], предлагается в процедуре вычисления элементов $\mathbf{Z}_1$ и $\mathbf{Z}_2$ открытого ключа дополнительно использовать операцию скалярного умножения на секретные значения. Кроме того, для обеспечения потенциальной возможности реализации алгоритма ЭЦП с использованием коммутативной КАА с мультипликативной группой, обладающей трехмерной цикличностью, вместо маскирующих векторных множителей **D** и **U** предлагается использовать принадлежащие одной циклической группе множители **D** и $\mathbf{D}^w$, где $w$ — секретное значение.

В предложенном способе получаем следующую процедуру генерации открытого ключа.

- Сгенерировать случайные векторы **G**, **Q**, и **D**, порядок каждого из которых равен одному и тому же простому числу $q$.
- Сгенерировать случайные натуральные числа $x < q$ и $w < q$ и вычислить векторы

$$\mathbf{Y}_1 = \mathbf{G}^x\mathbf{D} \text{ и } \mathbf{Y}_2 = \mathbf{Q}^x\mathbf{D}. \qquad (1)$$

- Сгенерировать случайные натуральные числа $\alpha < p$ и $\beta < p$ и вычислить векторы

$$\mathbf{Z}_1 = \mathbf{G}\mathbf{D}^w\alpha \text{ и } \mathbf{Z}_2 = \mathbf{Q}\mathbf{D}^w\beta. \qquad (2)$$

Открытым ключом являются две пары векторов: ($\mathbf{Y}_1$, $\mathbf{Z}_1$) и ($\mathbf{Y}_2$, $\mathbf{Z}_2$). Личным секретным ключом владельца этого открытого ключа является набор значений $x$, $w$, **G**, **Q** и **D**. Далее рассмотрим процедуры генерации и проверки подлинности подписи в схеме ЭЦП с открытым ключом, вычисленным по предложенному способу.

### Разработанная схема ЭЦП

Пусть дан электронный документ $M$, к которому надо сформировать цифровую подпись владельца открытого ключа ($\mathbf{Y}_1$, $\mathbf{Z}_1$) и ($\mathbf{Y}_2$, $\mathbf{Z}_2$), сгенерированного по формулам (1) и (2). Процедура генерации подписи имеет следующий вид.

- Сгенерировать четыре случайных натуральных числа $k < q$, $t < q$, $\rho_1 < p$ и $\rho_2 < p$.
- Вычислить два вектора-фиксатора $\mathbf{V}_1$ и $\mathbf{V}_2$ по следующим формулам:

$$\mathbf{V}_1 = \mathbf{G}^k\mathbf{D}^t\rho_1 \text{ и } \mathbf{V}_2 = \mathbf{Q}^k\mathbf{D}^t\rho_2.$$

- Вычислить значение $e = f_h(M, \mathbf{V}_1, \mathbf{V}_2)$ (первый элемент ЭЦП).
- Вычислить значение $s = k - ex \bmod q$ (второй элемент ЭЦП).
- Вычислить значение $d = t - e - ws \bmod q$ и вектор $\mathbf{S} = \mathbf{D}^d$ (третий элемент ЭЦП).
- Вычислить значение $\sigma_1 = \rho_1\alpha^{-s} \bmod p$ (четвертый элемент ЭЦП).
- Вычислить значение $\sigma_2 = \rho_2\beta^{-s} \bmod p$ (пятый элемент ЭЦП).

На выходе этого алгоритма получаем цифровую подпись в виде набора из пяти элементов $(e, s, \sigma_1, \sigma_2, \mathbf{S})$. Основной вклад в вычислительную сложность алгоритма $W$ вносят операции возведения в степень в рассматриваемой четырехмерной алгебре, т. е. можно принять оценку $W = 5$ операций экспоненцирования.

Алгоритм проверки набора $(e, s, \sigma_1, \sigma_2, \mathbf{S})$ как подлинной подписи к документу $M$ включает следующие шаги.

- Используя открытый ключ, а именно две пары векторов ($\mathbf{Y}_1$, $\mathbf{Z}_1$) и ($\mathbf{Y}_2$, $\mathbf{Z}_2$), вычислить векторы $\tilde{\mathbf{V}}_1 = \mathbf{Y}_1^e\mathbf{S}\mathbf{Z}_1^s\sigma_1$ и $\tilde{\mathbf{V}}_2 = \mathbf{Y}_2^e \circ \mathbf{S} \circ \mathbf{Z}_2^s\sigma_2$.
- Присоединив к документу векторы $\tilde{\mathbf{V}}_1$ и $\tilde{\mathbf{V}}_2$, вычислить значение хэш-функции $\tilde{e} = f_h\left(M, \tilde{\mathbf{V}}_1, \tilde{\mathbf{V}}_2\right)$.
- Проверить выполнимость равенства $\tilde{e} = e$. Если оно справедливо, то ЭЦП $(e, s, \sigma_1, \sigma_2, \mathbf{S})$ считается подлинной. Если $\tilde{e} \neq e$, то подпись $(e, s, \sigma_1, \sigma_2, \mathbf{S})$ отклоняется.

Вычислительная сложность алгоритма проверки подлинности ЭЦП равна $W = 4$ операций экспоненцирования.

Демонстрация корректности работы рассмотренной схемы ЭЦП предполагает выполнение доказательства того, что вычисленная владельцем открытого ключа подпись успешно проходит процедуру проверки подлинности подписи. Пусть подпись $(e, s, \sigma_1, \sigma_2, \mathbf{S})$ получена в соответствии с процедурой генерации подписи при использовании правильного личного секретного ключа под-

писанта. Тогда, подавая на вход проверочной процедуры подпись $(e, s, \sigma_1, \sigma_2, \mathbf{S})$, имеем следующее доказательство корректности работы предложенной схемы подписи:

$$\tilde{\mathbf{V}}_1 = \mathbf{Y}_1^e \mathbf{S} \mathbf{Z}_1^s \sigma_1 = \left(\mathbf{G}^x \circ \mathbf{D}\right)^e \mathbf{D}^d \left(\mathbf{G}\mathbf{D}^w \alpha\right)^s \rho_1 \alpha^{-s} =$$
$$= \mathbf{G}^{xe+s} \mathbf{D}^{e+d+ws} \rho_1 = \mathbf{G}^k \mathbf{D}^t \rho_1 = \mathbf{V}_1;$$

$$\tilde{\mathbf{V}}_2 = \mathbf{Y}_2^e \circ \mathbf{S} \circ \mathbf{Z}_2^s \sigma_2 = \left(\mathbf{Q}^x \circ \mathbf{D}\right)^e \mathbf{D}^d \left(\mathbf{Q}\mathbf{D}^w \beta\right)^s \rho_2 \beta^{-s} =$$
$$= \mathbf{Q}^{xe+s} \mathbf{D}^{e+d+ws} \rho_2 = \mathbf{Q}^k \mathbf{D}^t \rho_2 = \mathbf{V}_2 \Rightarrow$$
$$\Rightarrow \tilde{e} = f_h\left(M, \tilde{\mathbf{V}}_1, \tilde{\mathbf{V}}_2\right) = f_h\left(M, \tilde{\mathbf{V}}_1, \tilde{\mathbf{V}}_2\right) = e.$$

Рассмотрим следующие отношения элементов открытого ключа:

$$\mathbf{Y}_1 \mathbf{Y}_2^{-1} = \mathbf{G}^x \mathbf{Q}^{-x} = (\mathbf{G}\mathbf{Q}^{-1})^x;$$
$$\mathbf{Z}_1 \mathbf{Z}_2^{-1} = (\mathbf{G}\mathbf{Q}^{-1})\, \alpha\beta^{-1}.$$

Видно, что векторы $\mathbf{Y}_1\mathbf{Y}_2^{-1}$ и $\mathbf{Z}_1\mathbf{Z}_2^{-1}$ принадлежат различным циклическим группам, содержащимся в мультипликативной группе четырехмерной коммутативной КАА, использованной в качестве алгебраического носителя. Таким образом, благодаря использованию различных скалярных множителей при вычислении элементов открытого ключа $\mathbf{Z}_1$ и $\mathbf{Z}_2$ устраняется недостаток, присущий схеме ЭЦП [10]. Однако применение различных скалярных множителей потребовало использования двух дополнительных элементов подписи, используемых в различных проверочных уравнениях.

Последний момент показывает, что класс схем ЭЦП с удвоенным проверочным уравнением может быть расширен на случай использования только части элементов подписи в обоих уравнениях. Так, в предложенной схеме ЭЦП элементы $e$, $s$ и $\mathbf{S}$ входят в каждое проверочное уравнение, элемент $\sigma_1$ используется только в первом, а $\sigma_2$ — во втором проверочном уравнении.

## Заключение

Прием удвоения проверочного уравнения представляет интерес для реализации постквантовых схем ЭЦП, основанных на СЗДЛ и использующих коммутативную КАА в качестве алгебраического носителя. Выполненное исследование показывает, что коммутативные КАА предоставляют достаточно разнообразные возможности по разработке схем ЭЦП, основанных на СЗДЛ. Разработка на основе предложенного способа схемы ЭЦП на трехмерной коммутативной КАА представляет практический интерес в связи с потенциальной возможностью существенного повышения производительности процедур генерации и проверки подлинности подписи. Эта задача составляет предмет самостоятельной работы, включающей разработку трехмерных КАА с мультипликативной группой, обладающей трехмерной цикличностью.

*Работа выполнена при финансовой поддержке бюджетной темы № 0060-2019-0010.*

**Литература**


1. *Молдовян П. А., Морозова Е. В., Молдовян Д. Н., Пилькевич С. В.* Повышение производительности процедур коммутативного шифрования // Вопросы защиты информации. 2009. № 4. С. 24—31.
2. *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.
3. *Молдовян Д. Н.* Конечные некоммутативные группы как примитив криптосистем с открытым ключом // Информатизация и связь. 2010. № 1. С. 61—65.
4. *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.
5. *Молдовян Н. А., Абросимов И. К.* Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23—32.
6. *Молдовян Д. Н., Молдовян А. А.* Постквантовая схема открытого распределения ключей // Вопросы защиты информации. 2020. № 4. С. 3—10.
7. *Moldovyan D. N.* New Form of the Hidden Logarithm Problem and Its Algebraic Support // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2020. № 2(93). P. 3—10.
8. *Молдовян Д. Н.* Задание шестимерных алгебр как носителей криптосхем, основанных на скрытой задаче дискретного логарифмирования // Вопросы защиты информации. 2021. № 1. С. 26—32. DOI: 10.52190/2073-2600_2021_1_26.
9. *Moldovyan D.N.* A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. V. 27. № 2. P. 293—308.
10. *Moldovyan D. N., Moldovyan A. A., Moldovyan N. A.* A novel method for development of post-quantum digital signature schemes // Информационно-управляющие системы. 2020. № 6. С. 21—29. DOI:10.31799/1684-8853-2020-6-21-29.
11. *Moldovyan N. A.* Fast signatures based on non-cyclic finite groups // Quasigroups and Related Systems. 2010. V. 18. № 1. P. 83—94.
12. *Moldovyan 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.
13. *Moldovyan N. A., Moldovyan A. A.* Candidate for practical post-quantum signature scheme // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16. Вып. 4. С. 455—461. https://doi.org/10.21638/11701/spbu10.2020.410.

# Post-quantum digital signature algorithm on commutative algebra

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

*A new method for developing post-quantum digital signature schemes on commutative algebras, multiplicative group of which has multidimensional cyclicity, is proposed. The method is based on the technique of doubling the verification equation. Novelty is the combination of vector and scalar multiplication when generating a public key. A computationally difficult problem used in the proposed method is assigned to the type of a hidden discrete logarithm problem.*

*Keywords:* information security, post-quantum cryptography, finite associative algebra, commutative algebra, multidimensional cyclicity, digital signature, public key.

Bibliography — 13 references. *Received August 1, 2021*

# ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004:056:5.65:011:56.004:94.517:9.004:43
DOI: 10.52190/2073-2600_2021_3_45

## Модель определения затрат вычислительных ресурсов для развертывания интегрированной системы безопасности

*К. В. Пителинский*, канд. техн. наук; *И. А. Простов*; *С. С. Амфитеатрова*
ФГАОУ ВО «Московский политехнический университет», Москва, Россия

*Д. А. Ермолатий*
ФГБОУ ВО «Российская академия народного хозяйства и государственной службы», Москва, Россия

*Рассмотрена проблема оценки ресурсов, необходимых для развертывания и функционирования интегрированной системы информационной безопасности (ИБ) предприятия/организации. В качестве ее решения предоставлена модель, позволяющая реализовать алгоритмы, которые могут быть заложены в будущую систему ИБ предприятия и позволят оценить потенциальные затраты ресурсов в ходе ее внедрения. Представлено разработанное для упрощения деятельности ЛПР веб-приложение, позволяющее быстро и наглядно получить необходимые данные из представленной модели (алгоритмически реализованное на языке программирования JavaScript). Основная цель данного веб-приложения — быстрое предоставление результата в виде наглядного графика работы численной модели с помощью интерактивного ввода пользователем необходимых модельных параметров.*

*Ключевые слова*: защита информации, информационная безопасность, интегрированная система безопасности, корпоративная информационная система, конкурентоспособность, непрерывность бизнес-процессов, численное моделирование, визуализация, дифференциальные уравнения, JavaScript, C++, C#.

В условиях постоянно ускоряющихся процессов информатизации предприятий и организаций в различных отраслях экономики все большую важность приобретает работа с информацией, получаемой из различных источников и используемой для обеспечения непрерывности реализуемых бизнес-процессов. Это ведет к получению прибыли и к поддержанию на должном уровне конкурентоспособности. Надо отметить, что эпидемия COVID-19 негативно повлияла как на деятельность предприятий/организаций, так и на жизнь обычных людей, наложив сильный отпечаток на обеспечение их информационной безопасности как субъектов экономических отношений (см. рис. 1 и 2 [1]), подвергаемых различного рода атакам и воздействиям злоумышленников (по данным компании Positive Technologies).

При постоянно увеличивающемся объеме обрабатываемой и хранимой информации из-за массового перехода на удаленный режим работы наиболее остро стоят вопросы сохранения ее конфиденциальности, целостности и доступности (в рамках классической модели информационной безопасности CIA) путем создания или развития существующей системы защиты информации. В таком случае руководству предприятия/организации для эффективного планирования требуется использовать максимально точные количественные модели, позволяющие оценить необходимые ресурсы (в том числе и вычислительные), которые необходимо затратить для построения такой системы.

**Пителинский Кирилл Владимирович**, доцент, MBA, доцент кафедры "Информационная безопасность".
E-mail: yekadath@gmail.com
**Простов Игорь Андреевич**, студент кафедры "Информационная безопасность".
E-mail: igorprostoff@gmail.com
**Амфитеатрова Софья Сергеевна**, студент кафедры "Информационная безопасность".
E-mail: piacanlie@gmail.com
**Ермолатий Денис Александрович**, аспирант Института экономики, математики и информационных технологий.
E-mail: denis.yermolatiy@yandex.ru

*Статья поступила в редакцию 28 июня 2021 г.*

© Пителинский К. В., Простов И. А., Амфитеатрова С. С., Ермолатий Д. А., 2021

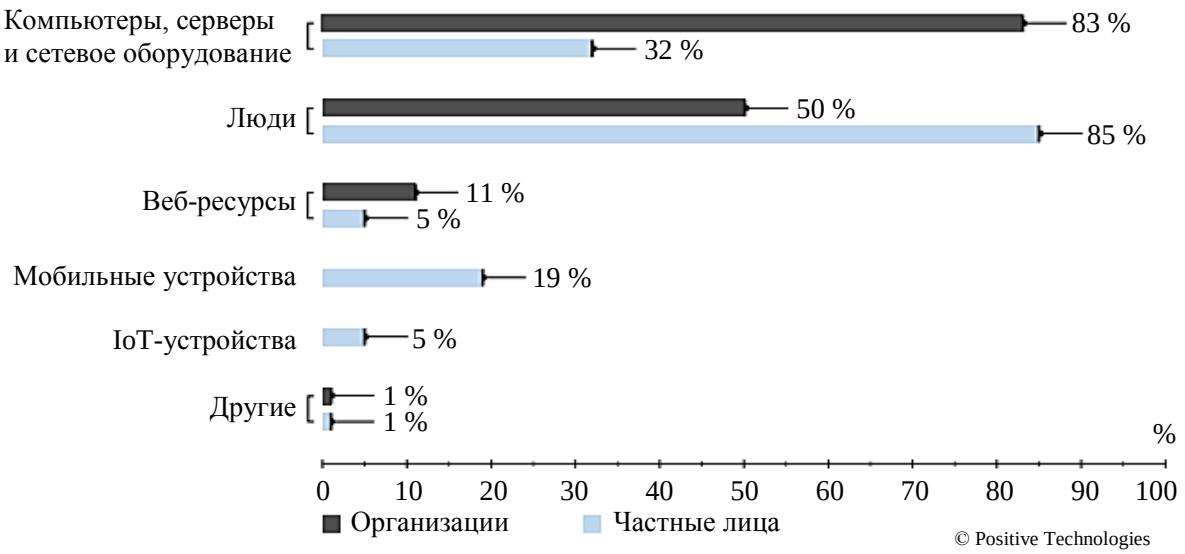



***Рис. 1. Объекты атак (доля атак на IV квартал 2020 г.)***

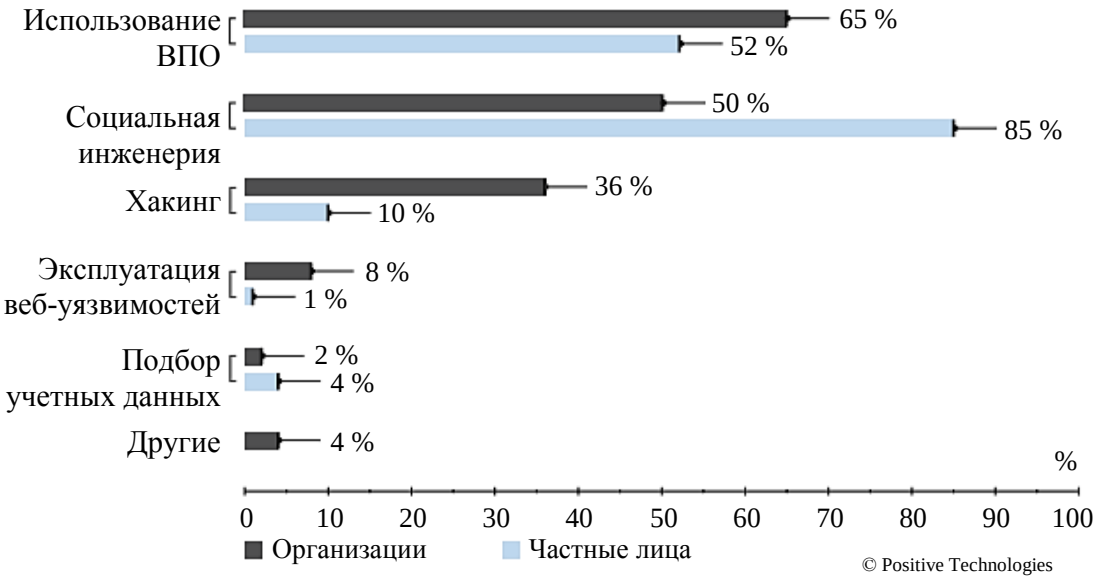



***Рис. 2. Методы атак (доля атак на IV квартал 2020 г.)***

Эффективная система менеджмента непрерывности бизнеса согласно ISO 22301:2019 должна соответствовать определенному списку требований для обеспечения комплексной защиты от инцидентов информационной безопасности (ИБ), а также процессов по снижению вероятности их реализации, обеспечению ответных мер и восстановления корпоративной информационной системы (КИС) в период после реализации инцидентов. В свою очередь, каждый процесс, который существует в этой системе, по истечению некоторого времени перестает быть эффективным. Если такие процессы вовремя не модифицировать, то производственно-технологическая система начнет деградировать по своим функциональным характеристикам.

Для обеспечения ИБ предприятия/организации, как правило, выстраивают свои интегрированные системы безопасности (ИСБ), состоящие из множества функциональных подсистем, каждая из которых выполняет свою функцию (рис. 3). Каждое предприятие/организация, ставящее перед собой задачу построения ИСБ, сталкивается с проблемой рационального выделения финансов для этого процесса. Особую сложность представляют ситуации, когда интегрированная система безопасности строится "с нуля". Тогда представление о том, какие компоненты должны присутствовать в системе и какие задачи она будет решать, могут отсутствовать. Здесь можно прибегнуть к средствам численного моделирования.

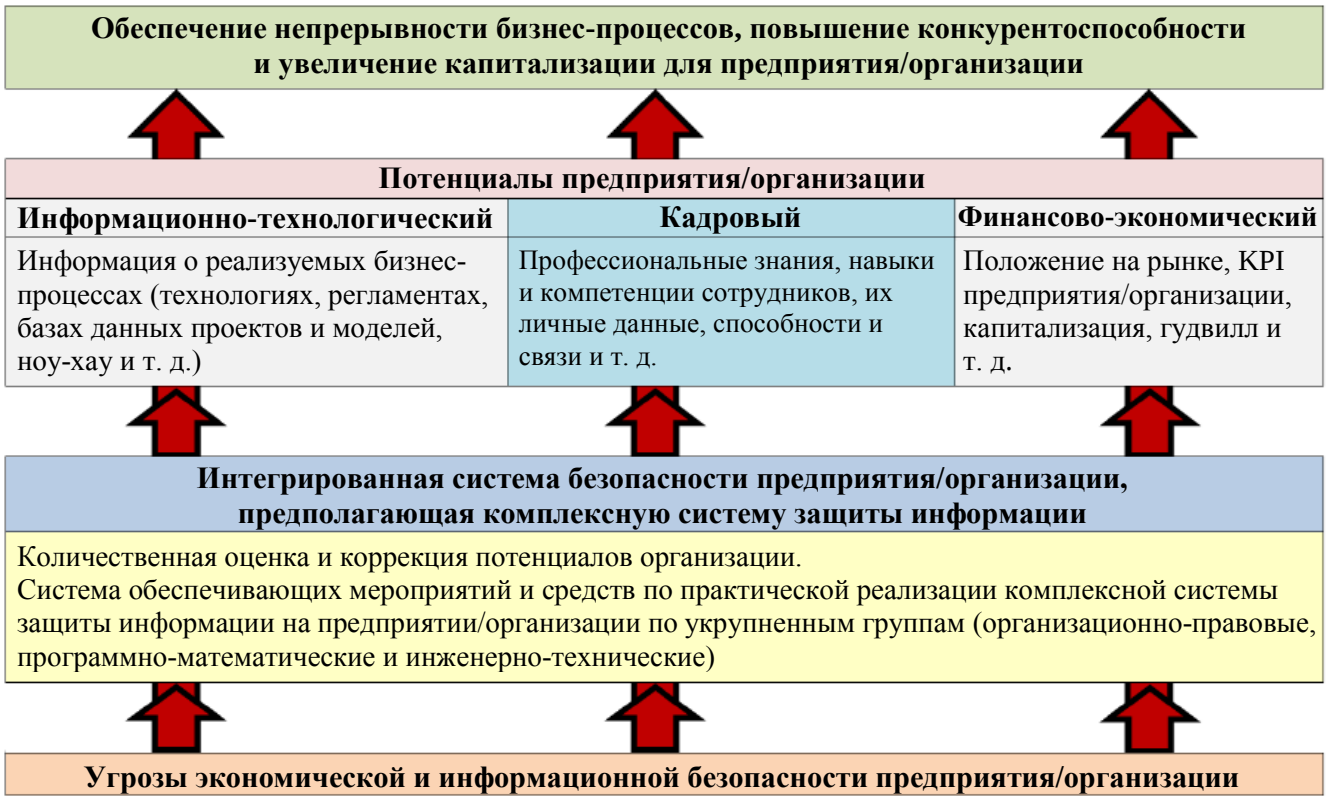



***Рис. 3. Укрупненная схема функционирования ИСБ предприятия/организации (предложена К. В. Пителинским)***

С помощью численного моделирования можно реализовать алгоритмы, которые потенциально будут заложены в будущую ИСБ предприятия/организации, и достаточно точно оценить затраты на её построение. Такой подход проще, чем использование математических средств моделирования. Кроме того, он позволяет не проводить эксперименты на реальных объектах, что является достаточно большим преимуществом при планировании будущей интеграционной системы безопасности. При использовании математического (а при необходимости и имитационного) моделирования требуется определить все алгоритмы, которые будут применяться в системе, а также желаемые и фактические метрики эффективности проектируемой системы ИСБ.

### Модель развертывания ИСБ

Как уже говорилось, одним из важнейших факторов, которые необходимо учитывать при построении ИСБ, является вопрос об объемах и стоимости выделяемых ресурсов. Для решения данной проблемы можно воспользоваться методом численного моделирования, подобным использованному в [2]. Полученные данные помогут оценить, какой объем ресурсов потребуется для построения системы и через какое время эти вложения окупятся.

Обозначим через $y(t)$ фактическое значение интегральной метрики (показателя) ИБ предприятия/организации [3, 4] на существующей вычислительной мощности в составе ИСБ (развернутые и функционирующие службы, сетевые сканеры, мониторы ИБ и т. д.) на момент времени $t$. Предположим, что в дальнейшем прирост метрики уровня ИБ объема вычислений пропорционален остаточной вычислительной мощности КИС предприятия/организации.

Тогда

$$\Delta y = \gamma\left(x - y\right)\Delta t,$$

где $x = \text{const}$.

Исходя из этого получаем

$$T\frac{dy}{dt} + y = x;$$

$$T = \frac{1}{\gamma};$$

$$y\left(0\right) = y_0;\ y_0 < x.$$

Окончательно имеем

$$y\left(t\right) = x + \left(y_0 - x\right)e^{-1/T}.$$

При $y_0 = 0$ данное уравнение имеет следующее решение:

$$y(t) = x\left(1 - e^{-1/T}\right) \rightarrow y(T) = x\left(1 - e^{-1}\right),$$

где $T$ — временной промежуток, за который переходный процесс совершает основную часть своего пути от 0 до $x$.

Переходный процесс освоения вычислительных мощностей ИБС завершается ее выходом на заданное значение мощности (характеризуемое заданным значением ее интегральной метрики ИБ):

$$\lim_{t \to \infty} y(t) = x.$$

Для упрощения моделирования процесса построения ИСБ и освоения вычислительных мощностей КИС разработано веб-приложение, которое позволяет пользователю ввести основные данные и получить график, который будет отображать динамику развертывания СИБ (см. рис. 4).

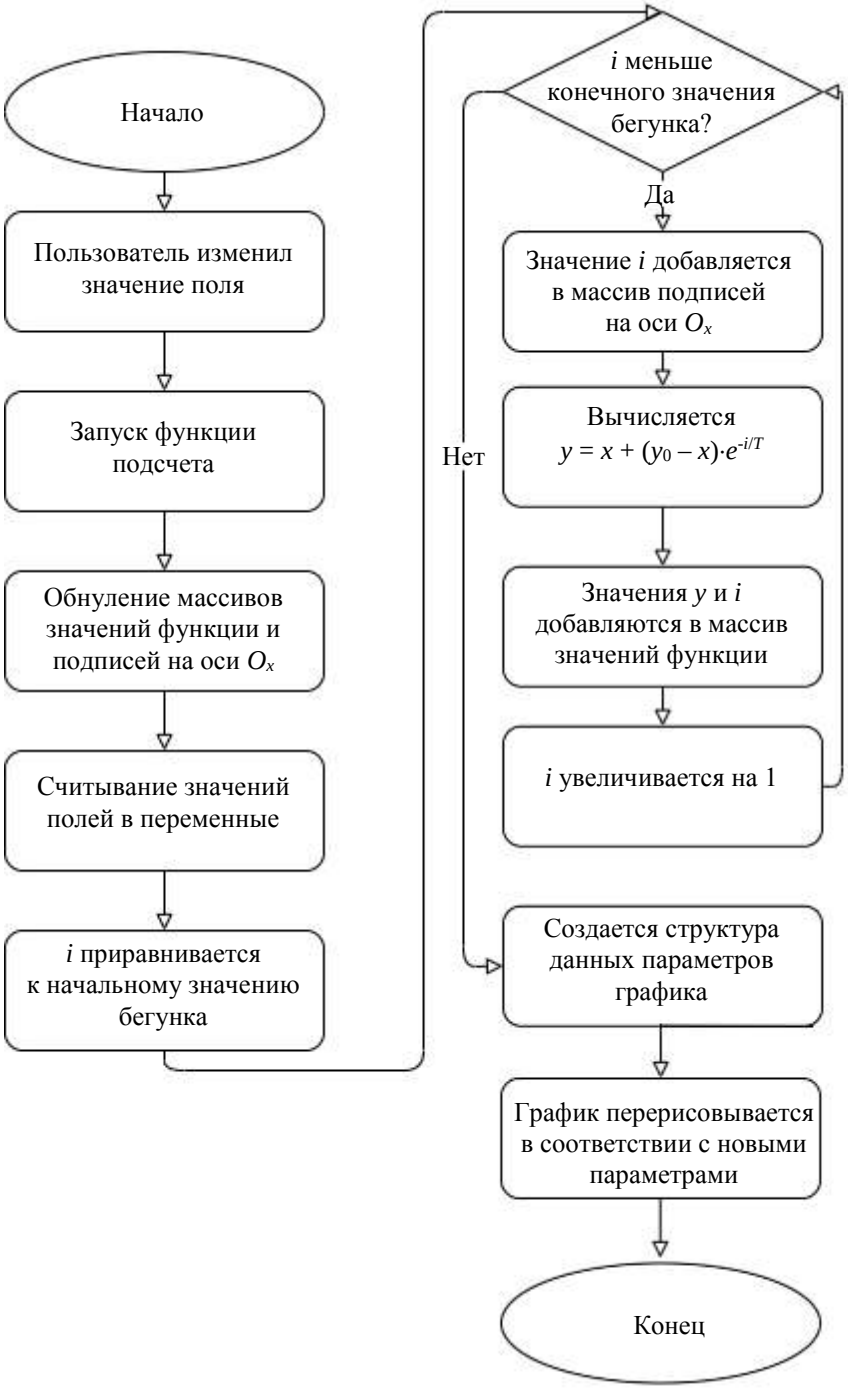



***Рис. 4. Алгоритм работы дискретной модели***

### Выбор среды алгоритмической реализации модели

При разработке приложения для численного моделирования проанализировано несколько платформ разработки и языков программирования (ЯП). В ходе сравнительного анализа получены результаты, приведенные в таблице.

Принцип работы ЯП C++ заключается в том, что код сначала записывается в файлы с расширением .cpp. Затем файлы .cpp компилируются. Компилятор преобразует код C++ в машинный код, который и выполняется на устройстве. Поэтому ЯП C++ очень близок к аппаратному обеспечению устройств. Это делает C++ чрезвычайно быстрым и идеальным для приложений реального времени. Компилятор ЯП здесь является компонентом, зависящим от операционной системы (ОС) и процессора. Компилятор зависит от устройства, следовательно, и ЯП C++ зависит от устройства.

Однако это означает, что код может работать только в ОС (и процессоре), совместимой с компилятором, который использовался для компиляции кода. Например, если компилятор Windows использовался на устройстве с ОС Windows для компиляции кода, то создается машинный код для ОС Windows.

Если для компиляции кода C++ используется компилятор ОС Linux, то скомпилированный код может работать только на устройстве с ОС Linux. Иногда некоторые модули/пакеты C ++ совместимы не со всеми ОС.

В свою очередь, JS — это интерпретируемый ЯП. Принцип работы ЯП JS заключается в том, что сначала создается или устанавливается файл его исходного кода. Если требуется выполнить код на ЯП JS, он будет интерпретирован во время выполнения исполняемым файлом ("движком") JS, установленным в ОС (либо внутри другого программного обеспечения, например браузера). Следует отметить, что можно написать код на ЯП JS в одной ОС, скопировать его в другую ОС и просто запустить.

Код ЯП C# работает схожим с ЯП C++ образом: он также компилируется, но не в машинные команды, как в случае с ЯП C++, а в специальный байт-код, который позже исполняется виртуальной машиной .NET, установленной в ОС (аналогично "движку", который требуется для работы JS).

Для ЯП C++ требуется скомпилировать код для каждой ОС заранее. Именно это отличие делает ЯП C++ чрезвычайно быстрым по сравнению с ЯП JS (который является интерпретируемым языком и выполняется медленнее, чем C++). Промежуточным по скорости является ЯП C#. Его байт-код выполняется быстрее, чем выполняются интерпретируемые команды ЯП JS.

**Сравнение ЯП, пригодных для реализации модели**

| C++ | JS (JavaScript) | C# |
|---|---|---|
| Сложность кода сравнима с ЯП, основанным на C, но он более строг в сравнении с JS | Самый простой в написании код из-за простого синтаксиса, похожего на ЯП C++, но с некоторыми допущениями | Сложность кода находится на уровне ЯП C++ |
| Большой объем кода | Объем кода немного меньше (в сравнении с ЯП C# или C++) | Большой объем кода |
| Требуется статическое присвоение типа объявленной переменной | Не требуется предварительного объявления переменной или ее типа для ее использования | Требуется статическое присвоение типа объявленной переменной |
| Компилируемый ЯП | Интерпретируемый ЯП | Компилируемый в байт-код, ЯП для исполнения требуется .NET Framework |
| Содержит 52 ключевых слова (предопределенных зарезервированных идентификатора) | Содержит 64 ключевых слова | Содержит 77 ключевых слов |
| "Гибридный" ЯП, поддерживает и процедурное и объектно-ориентированное программирование | Поддерживает ряд парадигм программирования (объектно-ориентированное, процедурное, функциональное программирование и т. д.) | Поддерживает множество парадигм программирования (объектно-ориентированное, процедурное, функциональное программирование и т. д.) |
| Поддерживает одиночное и множественное наследование | Поддерживает два типа наследования: классическое и прототипное | Поддерживает только одиночное наследование |
| Используется оператор new для выделения динамической памяти и оператор delete для ее освобождения | Автоматическое выделение и освобождение памяти | Используются оператор new для выделения динамической памяти и автоматическое освобождение памяти |

JS — это ЯП высокого уровня (как и, условно, C++ и C#). Благодаря большему числу встроенных функций (выполнение которых обеспечивает "движок", например выделение памяти) и различных библиотек ЯП JS прост и понятен. Это его значительное преимущество, которое ведет к тому, что все больше и больше разработчиков начинает применять ЯП JS во все большем числе сфер (фроненд- и бэкенд-разработка, создание мобильных приложений и т. д.).

Однако языки ЯП C++ и ЯП C# являются приоритетными, если необходимо разработать приложение, требовательное к скорости работы и строго привязанное к конкретной ОС.

Так как для разработки приложения требовалось сохранить возможность его использования в различных ОС, был выбран ЯП JS для исполнения в веб-интерфейсе приложения. Исходный код расчета функции приведен на рис. 5.

```
$(document).ready(function () {
    var data = []
    var ctx = document.getElementById('myChart').getContext('2d');
    var myChart = new Chart(ctx, {
        type: 'line',
        data: {
            labels: [],
            datasets: [{
                label: 'y(t)',
                data: [],
                backgroundColor: ['rgba(255, 99, 132, 0.2)'],
                borderColor: ['rgba(255, 99, 132, 1)'],
                borderWidth: 1,
                fill: false
            }]
        },
        options: {
            fill: false
        }
    });
    $('input').on('change', function () {
        var labelsData = []
        var canvasData = []
        yzero = parseFloat($('#y0').val())
        x = parseFloat($('#x').val())
        T = parseFloat($('#T').val())
        xstart = parseFloat($('#rangeStart').val())
        xstop = parseFloat($('#rangeStop').val())
        for (let i = xstart; i < xstop; i++) {
            labelsData.push(i)
            var y = x + (yzero - x) * Math.pow(Math.E, -i / T)
            canvasData.push({ x: i, y: y })
        }
        var chartData =
        {
            labels: labelsData,
            datasets: [{
                label: 'Цифры',
                data: canvasData,
                backgroundColor: ['rgba(255, 99, 132, 0.2)' ],
                borderColor: ['rgba(255, 99, 132, 1)'],
                borderWidth: 1,
                fill: false
            }]
        } 
        myChart.data = (chartData);
        myChart.update();
    })
})
```

***Рис. 5. Расчет функции на ЯП JS***

Результаты работы программы через веб-интерфейс представлены на рис. 6 и 7.

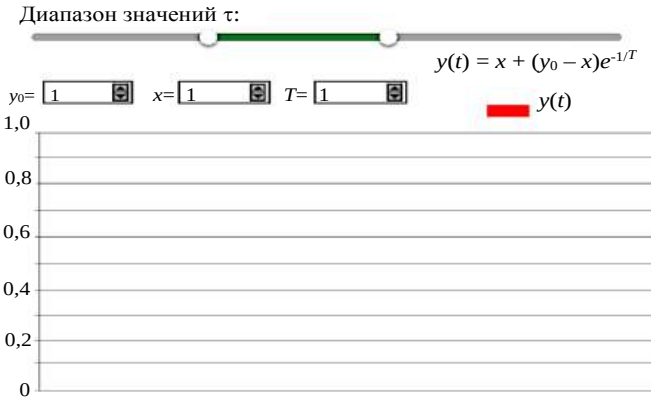



***Рис. 6. Вид интерфейса программы после инициализации***

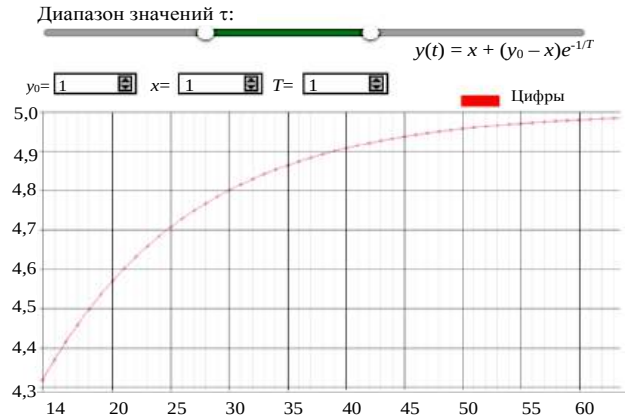



***Рис. 7. Расчет функции y(t) по введенным значениям и вывод ее графика***

**Заключение**

Из вычислительного эксперимента видно, что полученная численная модель и ее программная реализация могут значительно упростить лицу, принимающему решения (офицеру безопасности), процедуры расчета необходимых объемов ресурсов, требуемых для построения полноценно действующей системы защиты информации на предприятии/организации.

**Литература**


1. Актуальные киберугрозы: IV квартал 2020 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q4/ (дата обращения: 23.05.2021).
2. *Пителинский К. В.* Построение и эксплуатация интегрированной системы безопасности университетского комплекса // Специальная техника. 2009. № 6. С. 18—21.
3. Описание формы предоставления результатов оценки уровня информационной безопасности организаций банковской системы Российской Федерации [Электронный ресурс]. URL: https://www.altell.ru/legislation/standards/Form_discribe.pdf (дата обращения: 23.05.2021).
4. *Шаго Ф. Н.* Методика оценки эффективности системы менеджмента информационной безопасности по времени реакции системы на инциденты информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 4(92). https://cyberleninka.ru/article/n/metodika-otsenki-effektivnosti-sistemy-menedzhmenta-informatsionnoy-bezopasnosti-po-vremeni-reaktsii-sistemy-na-intsidenty (дата обращения: 23.05.2021).


# A model for determining the cost of computing resources for deploying an integrated security system


*K. V. Pitelinskiy, I. A. Prostov, S. S. Amfiteatrova*
Federal State Autonomous Educational Institution of Higher Education
"Moscow Polytechnic University", Moscow, Russia

*D. A. Ermolatiy*
Federal State Budgetary Educational Institution of Higher Education
"Russian Academy of National Economy and Public Administration", Moscow, Russia



*The problem of assessing the resources required for the deployment and operation of an integrated information security system of an enterprise/organization is considered. As its solution, a model is provided that allows you to implement algorithms that can be incorporated into the future information security system of an enterprise and will allow you to assess the potential cost of resources during its implementation. A web application developed to simplify the activities of decision makers is presented, which allows you to quickly and visually obtain the necessary data from the presented model (algorithmically implemented in the JavaScript programming language). The main goal of this web application is to quickly provide the result in the form of a visual graph of the numerical model using the interactive input of the necessary model parameters by the user.*



*Keywords*: information protection, information security, integrated security system, corporate information system, competitiveness, business continuity, numerical modeling, visualization, differential equations, JavaScript, C++, C#.

Bibliography — 4 references. *Received June 28, 2021*

УДК 004.73
DOI: 10.52190/2073-2600_2021_3_52

# Математическое моделирование как инструмент обоснования требований к характеристикам мер обеспечения технологической устойчивости информационных систем розничных сетей

*Е. В. Вайц*, канд. техн. наук; *В. М. Сычев*
ФГБОУВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», Москва, Россия

*Обоснована актуальность проблемы оценки характеристик мер обеспечения безопасности инфокоммуникационных технологий, используемых в бизнесе и электронной коммерции. Рассмотрены примеры функционального представления угроз несанкционированного доступа (НСД) к информации информационной системы розничной сети (ИС РС). Проиллюстрирована возможность формирования аргументированных требований к характеристикам средств защиты информации от НСД в ИС РС с использованием разработанных математических моделей.*

*Ключевые слова*: информационная система розничной сети (ИС РС), технологическая устойчивость ИС РС, эффективность реализации информационных процессов, эффективность предотвращения угрозы НСД к информации, технологический отказ.

Анализ существующих тенденций в развитии информатики как объективного начала жизнедеятельности общества и ее влияния на общественные процессы дает основание полагать, что основным направлением совершенствования информационных технологий является повышение качества информационной деятельности [1]. Характерным объектом, где указанная тенденция проявилась в полной мере, явились мобильные телекоммуникации, используемые в бизнесе и электронной коммерции [2].

Вместе с тем широкое внедрение информационных технологий в данную сферу деятельности, несмотря на очевидные преимущества, сопряжено с рядом негативных факторов [3]. Наиболее характерным отрицательным последствием информатизации коммерческой деятельности является рост уровня преступности в сфере мобильных телекоммуникаций, используемых в бизнесе и электронной коммерции. Указанная тенденция базируется как на постоянном совершенствовании способов и средств противоправных действий в данной сфере, так и на постоянном совершенствовании профессионализма криминальных структур в области информационных технологий [4].

**Вайц Екатерина Викторовна**, доцент кафедры "Защита информации".
E-mail: vaitcev@yandex.ru
**Сычев Владимир Михайлович**, старший преподаватель кафедры "Программное обеспечение ЭВМ и информационные технологии".
E-mail: vlr.sychev@gmail.com

*Статья поступила в редакцию 31 мая 2021 г.*

© Вайц Е. В., Сычев В. М., 2021

Анализ последствий такого рода криминальной деятельности дает основание утверждать, что ущерб, который несет среда информационной поддержки розничной торговли от подобного рода действий, как материальный, так и репутационный, существенен. Это является следствием объективно существующей уязвимости информации, хранимой и обрабатываемой в информационных системах розничных сетей.

В таблице приведены данные по инцидентам безопасности информации ИС РС компании Леруа Мерлен, выявленных дирекцией организации операций и модернизации информационных систем компании в 2020 г.

**Данные по инцидентам безопасности информации ИС РС компании Леруа Мерлен**

| Тип инцидента | Количество |
|---|---|
| Обнаружение индикатора компрометации Threat Intelligence | 652 |
| Включение отключенной учетной записи | 399 |
| Проверка на наличие индикаторов компрометации Threat Intelligence | 237 |
| Использование TOR на хосте | 227 |
| Отсутствие источника в профиле геолокации VPN | 188 |
| Внутреннее сканирование протоколов прикладного уровня | 134 |
| Попытка распределенного брутфорса | 131 |
| Аномальная вирусная активность | 114 |
| Внутреннее сетевое сканирование | 65 |
| Обнаружение сетевой атаки антивирусным программным обеспечением | 45 |
| Вирусная эпидемия | 43 |

*Окончание табл.*

| Тип инцидента | Количество |
|---|---|
| Добавление пользователя в критичные группы | 42 |
| Попытка подбора учетных записей к словарному паролю | 26 |
| Успешный административный доступ из сети Интернет | 20 |
| Установка новой системной службы | 9 |
| Изменение системного времени | 7 |
| Смена пароля для критичного пользователя | 5 |
| Создание и удаление учетной записи в течение короткого промежутка времени | 4 |
| Очистка журнала аудита | 4 |
| Удаление пользователя из критичной группы | 4 |
| Обнаружение нового сервиса во внешнем периметре | 3 |
| Длительное сканирование системы | 2 |
| Изменение политики аудита Windows | 2 |
| Создание пользователя с $ в имени учетной записи | 1 |
| **Общий итог** | **2364** |

Постоянное совершенствование методов несанкционированного доступа (НСД) к информационным ресурсам ИС РС как объекту противоправных действий, а также значительный ущерб коммерческой среде, наносимый такого рода действиями, обусловили целенаправленное системное исследование способов и средств защиты информации в этих системах и обеспечения их технологической устойчивости [5].

Вместе с тем высокая технологическая сложность механизмов обеспечения технологической устойчивости ИС РС относит вопросы их исследования к числу сложных как в научном, так и в практическом плане. Очевидно, что подобные исследования должны осуществляться всесторонне и системно [6] на основе адекватной оценки возможностей обеспечения технологической устойчивости ИС РС.

В соответствии с системным подходом исследование такой довольно специфичной информационной среды, как ИС РС, связано с решением проблемы оценки характеристик безопасности информации в ИС РС с достаточной степенью адекватности для обоснованности решений о направлениях совершенствования мер обеспечения их технологической устойчивости.

Необходимость решения данной проблемы обусловлена тем, что информационные объекты бизнес-среды относятся к объектам критической информационной инфраструктуры (КИИ). В соответствии с положениями п. статьи 12 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" "выработка мер по повышению устойчивости функционирования критической информационной инфраструктуры при проведении в отношении ее компьютерных атак" осуществляется на основе оценки безопасности критической информационной инфраструктуры [7].

Анализ существующих концепций оценки характеристик защищенности объектов информатизации, осуществляемый в рамках решения второй проблемы, дает основание утверждать, что достоинством этих концепций является простота процедур оценки. К недостаткам, принципиально ограничивающим их использование для адекватной оценки технологической устойчивости ИС РС, следует отнести отсутствие возможности учета динамики реагирования на угрозы НСД к информации этих систем, существенно зависящей от динамики воздействия такого рода угроз, и низкую статистическую достоверность, характерную для используемого в рамках этих концепций методического аппарата — аппарата экспертных оценок.

Устранение указанных недостатков влечет за собой необходимость разработки методического аппарата адекватной оценки технологической устойчивости ИС РС для обоснованности решений о направлениях совершенствования мер реагирования на угрозы НСД к информационным ресурсам этих систем.

Одним из наиболее распространенных путей обеспечения требования адекватности оценки функциональных характеристик исследуемых процессов является их детализация в рамках методологии функционального моделирования.

Общий вид функциональной модели целевой функции угрозы НСД к информации ИС РС приведен на рис. 1, а варианты моделей первого и второго уровней ее декомпозиции — на рис. 2 и 3 соответственно [8].

Формирование функциональной модели целевой функции "Защита информации от НСД в ИС РС" осуществляется как структурно идентичной, но противоположной по цели функции "НСД к информации ИС РС".

Функциональные модели угроз НСД к информации ИС РС и процессов защиты информации от такого рода угроз являются инструментом формализации этих процессов для математического представления их временных характеристик.

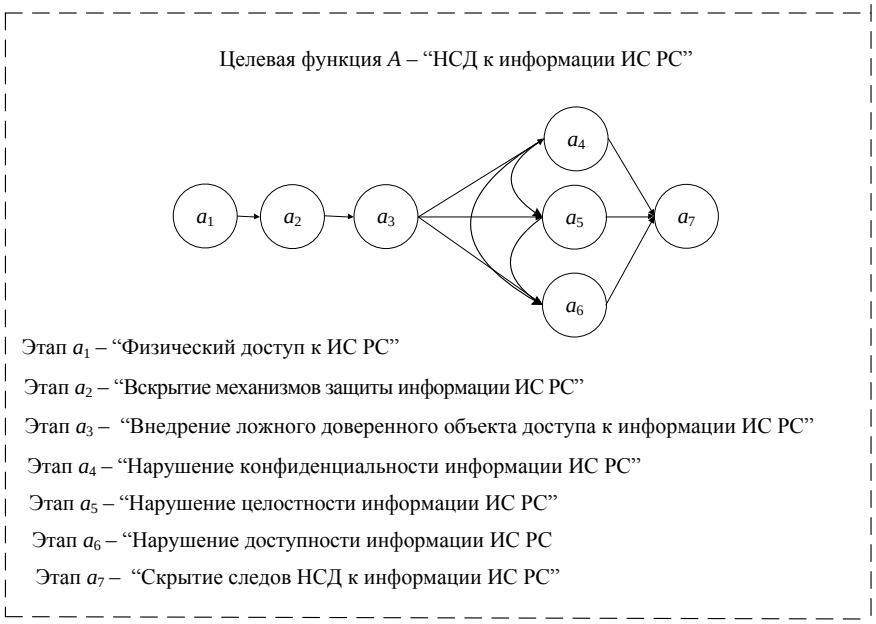



***Рис. 1. Функциональное представление целевой функции "НСД к информации ИС РС"***

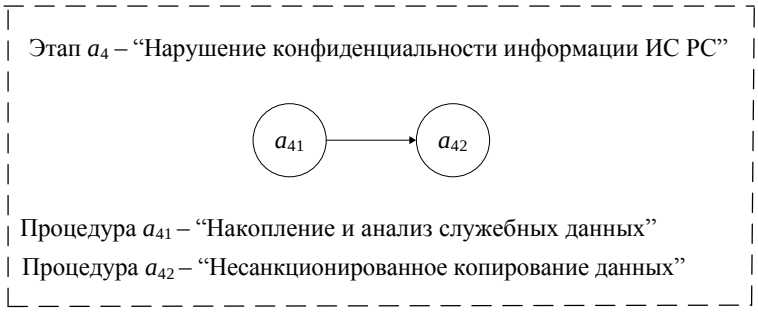



***Рис. 2. Функциональное представление этапа $a_4$ — "Нарушение конфиденциальности информации ИС РС"***

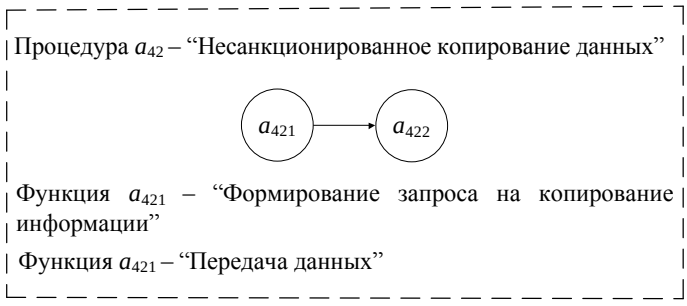



***Рис. 3. Функциональное представление процедуры $a_{42}$ — "Несанкционированное копирование данных"***

Математические модели позволяют определить согласно выражению [9]

$$\overline{\tau}(\alpha_k) = E\left[\tau(\alpha_1) * \tau(\alpha_2) * \ldots * \tau(\alpha_n) * \ldots * \tau(\alpha_N)\right] = \sum_{n=1}^{N} \overline{\tau}(\alpha_n) \quad (1)$$

средние значения времени реализации композиционно связанных функций $\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots, \alpha_N$.

В (1) $\overline{\tau}(\alpha_n)$ — среднее значение случайной величины времени $\tau(\alpha_n)$ реализации функции $\alpha_n$; $E(\ldots)$ — математическое ожидание композиции случайных величин; $*$— знак композиции случайных величин [10].

Полученные на основе (1) средние значения времени реализации этапов НСД к информации в ИС РС и времени реализации соответствующих мер ее защиты позволяют построить математическую модель показателя, характеризующего эффективность предотвращения такого рода действий. Условием эффективности здесь является неравенство

$$\tau_{(o)k} \le \overline{\tau}_k - \overline{\tau}_{(п)k}, \quad (2)$$

где $\tau_{(o)k}$ — время обнаружения угрозы реализации $k$-го этапа; $\overline{\tau}_k$ — среднее значение длительности $\tau_k$ этапа; $\overline{\tau}_{(п)k}$ — среднее значение времени

$\tau_{(\text{п})k}$ предотвращения угрозы; $k = 1, 2, \ldots, 7$ — индекс этапа, в соответствии с функциональным представлением целевой функции "НСД к информации ИС РС" (см. рис. 1).

Представив вероятность выполнения неравенства (1) в качестве показателя эффективности предотвращения угрозы реализации этапа, математическую модель данного показателя в общем виде запишем как

$$\begin{aligned}
&э_{(\text{п})k} = P\left(\tau_{(\text{о})k} \le \overline{\tau}_k - \overline{\tau}_{(\text{п})k}\right) = \\
&= \int_0^{t_k} dx \int_0^{x+\overline{\tau}_{ki}-\overline{\tau}_{(\text{п})k}} f_{1k}(y)\ f_{2i}(x)dy - \\
&- \int_0^{t_k} dx \int_0^{x} f_{1k}(y)\ f_{2i}(x)dy = \\
&= \int_0^{t_k} f_{2k}(x)\left[F_{1k}\left(x + \overline{\tau}_k - \overline{\tau}_{(\text{п})k}\right) - F_{1k}(0)\right]dx - \\
&- \int_0^{t_k} f_{2k}(t)\left[F_{1k}(x) - F_{1k}(0)\right]dx = \\
&= \int_0^{t_k} f_{2k}(x)\left[F_{1k}\left(x + \overline{\tau}_k - \overline{\tau}_{(\text{п})k}\right) - F_{1k}(x)\right]dx,
\end{aligned} \tag{3}$$

где $f_{2k}(x)$, $f_{1k}(y)$ — плотности распределения случайной величины времени $t_{(\text{в})k}$ возникновения угрозы реализации этапа и случайной величины времени $t_{(\text{о})k}$ ее обнаружения соответственно;

$F_{1k}(x)$ — функция распределения случайной величины $t_{(\text{о})k}$;

$t_k$ — время, в течение которого может быть реализован $k$-й этап.

Выразив время $t_{(\text{в})k}$ возникновения угрозы реализации этапа через время $t_{(\text{о})k}$ ее обнаружения и предположив, что он может быть реализован нарушителем в любой момент времени ($t_k \to \infty$), выражение (3) запишем в виде

$$э_{(\text{п})k} = \int_0^{\infty} f_{2k}(x)\left[F_{1k}(x + \overline{\tau}_k - \overline{\tau}_{(\text{п})k}) - F_{1k}(x)\right]dx. \tag{4}$$

Аналитическое выражение для показателя $S_k$ эффективности предотвращения угрозы реализации $k$-го этапа может быть получено путем подстановки в (4) выражений для плотности $f_{2k}(x)$ распределения случайной величины времени $t_{(\text{в})k}$ возникновения угрозы реализации этапа и функции $F_1(x)$ распределения случайной величины времени $t_{(\text{о})k}$ обнаружения такого рода угрозы, соответствующих законам распределения этих случайных величин.

Воспользовавшись потоковым представлением угроз НСД к информации ИС РС и свойствами стационарности, ординарности такого потока время $t_{(\text{в})k}$ возникновения угрозы реализации этапа представим как случайную величину, распределенную по экспоненциальному закону.

В свою очередь композиционный характер представления времени $t_{(\text{о})k}$ обнаружения угрозы дает основание рассматривать ее в соответствии с центральной предельной теоремой теории вероятностей (по Ляпунову и Линдебергу [11]) как случайную величину, распределенную по нормальному закону.

Для данного варианта законов распределения случайных величин математическая модель показателя эффективности предотвращения угрозы реализации $k$-го этапа НСД к информации ИС РС представляется как

$$\begin{aligned}
&э_{(\text{п})k} = \frac{1}{2}\exp\left[\frac{1}{2}\lambda\left(2\,\overline{\tau}_k + \sigma_k^2\,\lambda - 2\,\overline{\tau}_k - \overline{\tau}_{(\text{п})k}\right)\right] \times \\
&\times\left[1 - \operatorname{erf}\left(\frac{\overline{\tau}_k + \sigma_k^2\lambda - \overline{\tau}_{(\text{о})k} - \overline{\tau}_{(\text{п})k}}{\sigma_k\sqrt{2}}\right)\right] + \\
&+ \frac{1}{2}\operatorname{erf}\left(\frac{\overline{\tau}_k - \overline{\tau}_{(\text{о})k} - \overline{\tau}_{(\text{п})k}}{\sigma_i\sqrt{2}}\right) - \\
&- \frac{1}{2}\exp\left[\frac{1}{2}\lambda\left(\sigma_k^2\lambda - \overline{\tau}_{(\text{о})k} - \overline{\tau}_{(\text{п})k}\right)\right] \times \\
&\times\left[1 - erf\left(\frac{\sigma_k^2\lambda - \overline{\tau}_{(\text{о})k} - \overline{\tau}_{(\text{п})k}}{\sigma_k\sqrt{2}}\right)\right] + \\
&+ \frac{1}{2}\operatorname{erf}\left(\frac{\overline{\tau}_{(\text{о})k} + \overline{\tau}_{(\text{п})k}}{\sigma_k\sqrt{2}}\right),
\end{aligned} \tag{5}$$

где $\overline{\tau}_{(\text{о})k} = E(t_{(\text{о})k} - t_{(\text{в})k})$ — среднее значение случайной величины времени обнаружения выполняемых нарушителем действий по реализации им $k$-го этапа НСД к информации ИС РС;

$\sigma_k$ — среднеквадратическое отклонение случайной величины $\tau_{(\text{п})k}$;

$\lambda$ — плотность потока угроз НСД к информации ИС РС;

erf($x$) — функция ошибок [10].

Воспользовавшись поэтапным характером действий нарушителя по реализации угроз НСД к ин-

формации ИС РС, а также паузами в его действиях по завершению этих этапов, примем допущение о независимости соответствующих случайных событий. В этом случае выражение для показателя эффективности защиты информации от НСД в ИС РС представляется в виде

$$Э_{(з)} = 1 - \begin{bmatrix} (1 - э_{(п)1})(1 - э_{(п)2})(1 - э_{(п)3}) \times \\ \times (1 - э_{(п)4})(1 - э_{(п)5})(1 - э_{(п)6}) \times \\ \times (1 - э_{(п)7}) \end{bmatrix}. \quad (6)$$

В целях разработки математической модели показателя эффективности реализации информационных процессов в ИС РС определим соответствующее условие. Будем считать, что информационные процессы в ИС РС реализуются эффективно, если время реализации $\tau_{(р)}$ не превышает допустимое значение $\tau_{(д)}$, т. е. если выполняется неравенство

$$\tau_{(р)} \le \tau_{(д)}. \quad (7)$$

С учетом того, что $\tau_{(р)}$ в общем случае является случайной величиной, эффективность $Э_{(р)}$ реализации информационных процессов в ИС РС будет характеризоваться вероятностью выполнения условия (7), а соответствующий показатель будет представлен как

$$Э_{(р)} = P\left(\tau_{(р)} \le \tau_{(д)}\right). \quad (8)$$

Рассматривая (8) как функцию распределения вероятностей [10] случайной величины $\tau_{(р)}$, в качестве математической модели показателя $Э_{(р)}$ эффективности реализации информационных процессов в ИС РС можно использовать выражение

$$Э_{(р)} = P\left(\tau_{(р)} \le \tau_{(д)}\right) \approx P\left(\tau_{(р)} < \tau_{(д)}\right) = \int_0^{\tau_{(д)}} f_{(р)}(u)\,du, \quad (9)$$

где $f_{(р)}(u)$ — функция плотности вероятности случайной величины времени $\tau_{(р)}$ реализации информационных процессов в ИС РС.

Учитывая, что время реализации информационных процессов в ИС РС является характеристикой функциональной и определяется как композиция времен выполнения отдельных процедур накопления, обработки и обмена информацией в этих системах, а само множество этих процедур может достигать нескольких десятков, можно рассматривать случайную величину $\tau_{(р)}$ в соответствии с центральной предельной теоремой теории вероятностей [11] как распределенную по нормальному закону.

В этом случае выражение для определения показателя $Э_{(р)}$ эффективности реализации информационных процессов в ИС РС представляется в виде

$$Э_{(р)} = \mathrm{erf}\left(\frac{\tau_{(д)} - \overline{\tau}_{(р)}}{\sigma_{(р)}}\right), \quad (10)$$

где $\overline{\tau}_{(р)}$, $\sigma_{(р)}$ — среднее значение и среднеквадратическое отклонение случайной величины $\tau_{(р)}$ соответственно.

В свою очередь, среднее значение $\overline{\tau}_{(р)}$ времени $\tau_{(р)}$ реализации информационных процессов в ИС РС как математическая функция от целого ряда параметров, характеризующих процессы накопления, обработки и обмена информацией в этих системах, угрозы НСД к информации и меры ее защиты от подобного рода угроз, представляется в виде

$$\overline{\tau}_{(р)} = \overline{\tau}_{(ноо)} + \overline{\tau}_{(о)} + P_{(НСД)}\left(1 - Э_{(з)}\right)\overline{\tau}_{(вос)}, \quad (11)$$

где $\overline{\tau}_{(ноо)}$ — среднее значение случайной величины времени реализации процессов накопления, обработки и обмена информацией в ИС РС;

$\overline{\tau}_{(о)}$ — среднее значение случайной величины времени обнаружения угрозы НСД к информации в ИС РС, определяемое в соответствии с выражением

$$\overline{\tau}_{(о)} = \sum_{k=1}^{7} p_{(э)k}\,\overline{\tau}_{(о)k}; \quad (12)$$

$p_{(э)k}$ — вероятность реализации $k$-го ($k$ = 1, 2, …, 7) этапа действий нарушителя;

$P_{(НСД)}$ — вероятность угрозы НСД к информации ИС РС;

$\overline{\tau}_{(вос)}$ — среднее значение случайной величины времени $\tau_{(вос)}$ восстановления корректности процессов накопления, обработки и обмена информацией в ИС РС, подвергшихся угрозе НСД к информации.

В целях разработки математической модели показателя технологической устойчивости ИС РС определим соответствующее условие. Будем считать, что технологии накопления, обработки и обмена информацией в ИС РС реализуются устойчиво, если эффективность $Э_{(р)}(t)$ реализации информационных процессов в данной системе в динамике ее функционирования превышает уровень $Э_{(то)}$ технологического отказа (рис. 4), т. е. если выполняется неравенство

$$Э_{(р)}(t) > Э_{(то)}. \quad (13)$$

С учетом случайного характера динамики эффективности реализации информационных процессов в ИС РС (рис. 4) следует полагать, что $Э_{(р)}(t)$ в общем случае является случайной величиной. Тогда технологическая устойчивость $S_{(т)}$ ИС РС будет характеризоваться вероятностью выполнения условия (13), а соответствующий показатель будет представлен как

$$S_{(т)} = P\left(Э_{(р)}(t) > Э_{(то)}\right). \quad (14)$$

Если рассматривать (14) как функцию распределения вероятностей [10] случайной величины $Э_{(р)}(t)$, то в качестве математической модели показателя $S_{(т)}$ технологической устойчивости ИС РС можно использовать выражение

$$\begin{aligned} S_{(т)} &= P\left[Э_{(р)}(t) > Э_{(то)}\right] = \\ &= 1 - P\left[Э_{(р)}(t) \le Э_{(то)}\right] \approx \\ &\approx 1 - P\left[Э_{(р)}(t) < Э_{(то)}\right] = \int_0^{Э_{(то)}} f_{(р)}(w)\,dw, \end{aligned} \quad (15)$$

где $f_{(р)}(w)$ — функция плотности вероятности случайной величины $Э_{(р)}(t)$.

Учитывая, что динамика изменения эффективности реализации информационных процессов в ИС РС определяется динамикой угроз НСД к информации этих систем и формально описывается в терминах простейшего потока событий, можно рассматривать $Э_{(р)}(t)$ как случайную величину, распределенную по экспоненциальному закону.

В этом случае выражение (15) представляется в виде

$$S_{(т)} = \exp\left(-\frac{Э_{(то)}}{Э_{(р)}}\right), \quad (16)$$

где $Э_{(р)}$ определяется в соответствии с (10).

Разработанные математические модели позволяют решить весьма актуальную в практическом плане задачу — задачу обоснования требований к характеристикам мер обеспечения технологической устойчивости ИС РС (рис. 5).

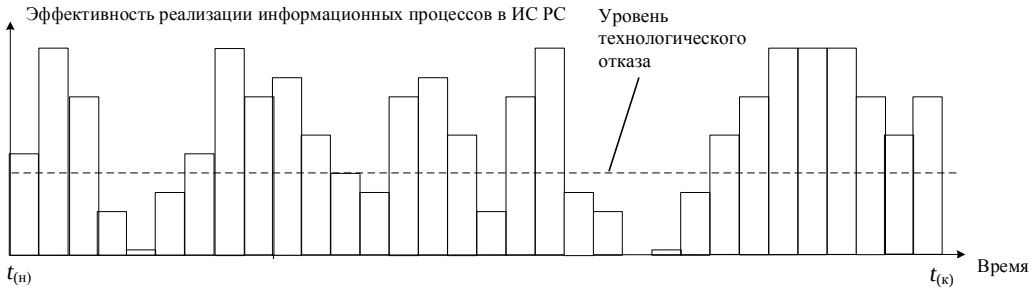



***Рис. 4. Динамика изменения эффективности реализации информационных процессов в ИС РС***

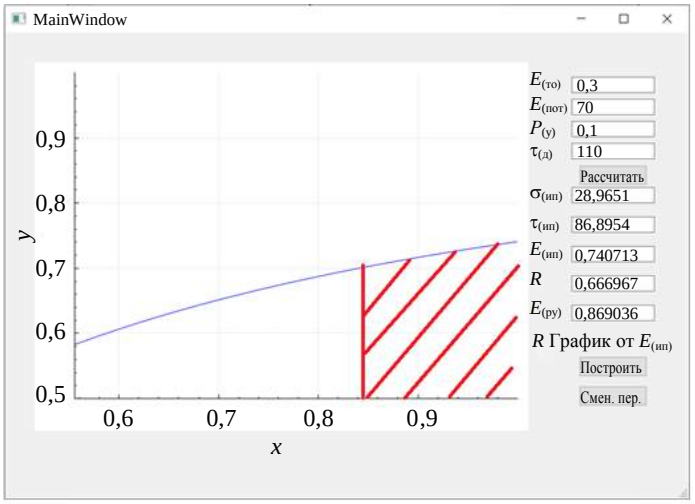



***Рис. 5. Зависимость технологической устойчивости ИС РС как математической функции от эффективности реализации информационных процессов***

## Заключение

Как следует из полученных результатов, заданный уровень технологической устойчивости ИС РС ($S_{(т)} = 0,7$) может быть достигнут, если средства защиты информации от НСД обеспечат уровень эффективности реализации информационных процессов не ниже 0,843.

Таким образом, очевидны возможности разработанных моделей как инструмента формирования обоснованных требований к характеристикам средств защиты информации от НСД.

**Литература**


1. *Скрыль С. В. и др.* Информатика: учебник для вузов МВД России. Информатика: Концептуальные основы. — М.: Маросейка, 2008. Т. 1. — 464 с.

2. *Гаврилов Л. П., Соколов С. В.* Мобильные телекоммуникации в электронной коммерции и бизнесе: учеб. пособие для студентов вузов, обучающихся по специальности "Коммерция" (торговое дело). — М.: Финансы и статистика, 2006. — 336 с.

3. *Запечников С. В. и др.* Информационная безопасность открытых систем: учебник для вузов. В 2 томах. Угрозы, уязвимости, атаки и подходы к защите. — М.: Горячая линия — Телеком, 2006. Т. 1. — 536 с.

4. *Скрыль С. В., Литвинов Д. В.* Использование существующего уровня информационных технологий в преступных целях // Вестник Воронежского института МВД России. 2007. № 3. С. 126—129.

5. *Андриянов В. В., Зефиров С. Л., Голованов В. Б., Голдуев Н. А.* Обеспечение информационной безопасности бизнеса. Изд. 2-е, перераб. и доп. — М.: Альпина Паблишерз, 2011. — 373 с.

6. *Скрыль С. В., Шелупанов А. А.* Основы системного анализа в защите информации: учеб. пособие для студентов вузов. — М.: Машиностроение, 2008. — 138 с.

7. Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". Принят Государственной Думой 12.07.2017. Одобрен Советом Федерации 19.07.2017 г.

8. *Скрыль С. В., Гайфулин В. В., Сычев В. М. и др.* Методические аспекты построения функциональной модели угроз несанкционированного доступа к компьютерной информации // Промышленные АСУ и контроллеры. 2019. № 11. С. 48—59.

9. *Скрыль С. В., Гайфулин В. В., Сычев В. М. и др.* Математические модели временных характеристик угроз несанкционированного доступа к компьютерной информации // Промышленные АСУ и контроллеры. 2019. № 11. С. 60—65.

10. *Вентцель Е. С.* Теория вероятностей: учебник. Изд. 11-е. — М.: КноРус, 2010. — 664 с.

11. *Коваленко И. Н., Филиппова А. Л.* Теория вероятностей и математическая статистика: учеб. пособие. Изд. 2-е, перераб. и доп. — М.: Высш. школа, 1982. — 256 с.


# Mathematical modeling as a tool for substantiating the requirements for the characteristics of measures to ensure the technological stability of information systems of retail chains


*E. V. Vaitc, V. M. Sychev*

Bauman Moscow State Technical University, Moscow, Russia



*The article substantiates the relevance of the problem of assessing the characteristics of security measures of information and communication technologies used in business and e-commerce. The examples of functional representation of threats of unauthorized access (NSD) to the information of the information system of the retail network (IS RS) are considered. The article illustrates the possibility of forming reasonable requirements for the characteristics of information security tools against NSD in the RS IS using the developed mathematical models.*



*Keywords*: information system of a retail network (IS RS), technological stability of IS RS, efficiency of implementation of information processes, efficiency of preventing the threat of unauthorized access to information, technological failure.

Bibliography — 11 references. *Received May 31, 2021*

# 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, следующих 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).