Индекс 79187

ISSN 2073-2600

# ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

1
(128)

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

Москва 2020

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

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


Межотраслевой научно-технический журнал

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

Подписной индекс **79379**

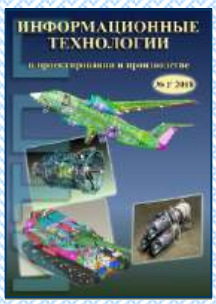
Издается с 1984 года


Межотраслевой научно-технический журнал

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

Подписной индекс **80089**

Издается с 1981 года

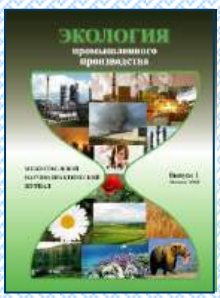



Научно-технический журнал

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

Подписной индекс **79378**

Издается с 1976 года




Межотраслевой научно-практический журнал

**Экология промышленного производства**
(4 выпуска)

Подписной индекс **80090**

Издается с 1993 года


Научно-практический журнал

**Вопросы защиты информации**
(4 выпуска)

Подписной индекс **79187**

Издается с 1974 года

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

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

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

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

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

# ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

**НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ**

**1 (128)**

**Москва 2020**
**Основан в 1974 г.**

## СОДЕРЖАНИЕ

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2020.
Вып. 1 (128). С. 1—72.

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

Подписано в печать 18.03.2020. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 8,4. Уч.-изд. л. 8,6.
Тираж 400 экз. Заказ 1947. Свободная цена.
Адрес редакции: 125424, Москва,
Волоколамское ш., 77. ФГУП «НТЦ оборонного комплекса «Компас».
http://ntckompas.ru
Отпечатано в ООО "РАПИТОГРАФ".
117342, Москва, ул. Бутлерова, д. 17Б.
Индекс 79187.

*К 75-летию Владимира Георгиевича МАТЮХИНА*
*генерала армии, доктора технических наук, действительного члена Академии криптографии РФ, Российской академии инженерных наук и Международной академии связи, лауреата Государственной премии РФ, первого заместителя генерального директора ОАО «НИИАС», главного редактора журнала "Вопросы защиты информации"*

Главному редактору нашего журнала Владимиру Георгиевичу Матюхину 4 февраля 2020 г. исполнилось 75 лет.

С 1969 г. по 2003 г. Владимир Георгиевич проходил военную службу в органах государственной безопасности, а с мая 1999 г. по март 2003 г. являлся генеральным директором ФАПСИ. В мае 2003 г. назначен первым заместителем министра обороны, исполняющим обязанности председателя государственного комитета Российской Федерации по оборонному заказу.

Под его научным руководством впервые был создан ряд крупномасштабных государственных интегрированных информационно-телекоммуникационных систем: защищенная система видеоконференцсвязи Президента Российской Федерации в федеральных округах, Ситуационный центр Президента Российской Федерации, информационно-телекоммуникационные системы в Аппарате Правительства РФ, Совете Федерации и Государственной думе Федерального собрания Российской Федерации, Конституционном, Высшем арбитражном судах России и других органах государственной власти и управления, в том числе региональные информационно-аналитические центры в субъектах России, ведомственные информационно-аналитические центры в министерствах и ведомствах.

С июня 2004 г. по февраль 2010 г. возглавлял Федеральное агентство по информационным технологиям (Росинформтехнологии, ФАИТ), внеся огромный вклад в развитие информационных технологий.

Каждый человек индивидуален. Каждый руководитель — тоже. С Владимиром Георгиевичем сработаться удается практически сразу. Работая на всех постах, он умелыми и ненавязчивыми подсказками направлял исследования и разработки в нужное для страны русло. В результате этих управляющих воздействий и были созданы инновационные системы, которые применялись на многих направлениях, включая кредитно-финансовую сферу и другие.

Под непосредственным руководством Владимира Георгиевича в ФАИТ было развито много важных направлений, получивших всеобщее признание, в том числе универсальная социальная карта (УСК) и ОГИЦ — общегосударственный информационный центр. Это масштабные проекты, прогремевшие на всю страну.

Созданием УСК занимался консорциум, включавший в себя научные, методические и промышленные предприятия. Основная идея заключалась в том, чтобы сделать универсальную СОЦИАЛЬНУЮ карту, включающую и финансовое приложение как одно из множества других. Огромное количество проблем должна была решить УСК, так как в разных регионах были разные льготы, субсидии, компенсации и т. д., и все это в очень непростых условиях почти полного отсутствия механизмов межбюджетных отношений. Эта работа была замечена и даже получила серьезное развитие, хотя и неожиданное: на основе идеологии УСК другими разработчиками была создана другая карта — универсальная электронная карта (УЭК). Вместе с тем логика УЭК была предложена новыми авторами совсем другой. Это была банковская карта с небольшим социальным приложением. Идея УСК была вывернута наизнанку, что и привело в скором времени к краху УЭК.

Идея ОГИЦ тоже намного опередила свое время и была не понята новым руководством отрасли. Только сейчас она пытается реинкарнировать то в виде «Гособлака», то в виде «ГЕОП» — государственной единой облачной платформы. А в те годы ОГИЦ уже функционировал, и на технические средства ОГИЦ было портировано немало функциональных систем электронного правительства России. Основы информационного общества закладывались уже тогда, и уже тогда можно было обеспечить мощный рывок вперед.

Конечно, этими направлениями не исчерпывались его работы. Было еще и многое другое: Академия криптографии, Ассоциация защиты информации, доверенная третья сторона — всего не перечислить.

Работая научным руководителем и первым заместителем директора НИИАС, одного из ведущих институтов РЖД, Владимир Георгиевич руководит созданием интеллектуальных систем управления движением. Немного стоит завидовать тем, кто сегодня получил возможность воспринимать и реализовывать идеи одного из выдающихся специалистов и руководителя в области информатизации и информационной безопасности.

Мы уверены, что впереди еще много блестящих идей и реализаций.
С юбилеем, Владимир Георгиевич!

**В. Конявский, зам гл. редактора, д-р. техн. наук,**
**заведующий кафедрой «Защита информации» МФТИ**

## 75 лет Владимиру Георгиевичу Матюхину

Долгие годы Владимир Георгиевич трудился на поприще разработки средств защиты информации (тогда еще в достаточно узком понимании этой тематики).

Не все можно сказать на страницах открытой печати, но вклад Владимира Георгиевича в развитие ранее очень закрытой, а теперь уже широко известной и находящейся на пике научно-технического развития тематики информационной безопасности весьма значим, что подтверждается его высокими научными и воинскими званиями.

Особо хочется отметить такие важные качества Владимира Георгиевича, как высокий уровень инженерной и математической подготовки, острое чувство нового и перспективного в технических вопросах, умение создавать трудоспособные коллективы, нацеленные на решение сложных научно-технических задач.

Владимиру Георгиевичу принадлежит идея создания уже хорошо известной Ассоциации защиты информации, и сделаны основополагающие шаги по ее становлению.

Опираясь на возможности этой Ассоциации, Владимиру Георгиевичу удалось поставить на прочную основу работу по совершенствованию в стране такой важной технологии, как электронная цифровая подпись, и одного из институтов ее практического применения — института удостоверяющих центров. Специально учрежденная для широкого обсуждения этой проблематики площадка «PKI-Форумов» ежегодно собирала на своих мероприятиях лучших специалистов страны, работающих в этой области. Личное участие Владимира Георгиевича в работе этого форума как руководителя ФАИТ придало данному мероприятию государственное звучание, а со временем и международный формат.

Сердечно поздравляю юбиляра. Несомненно, у Вас уважаемый Владимир Георгиевич, есть ряд интересных задумок и замыслов. Хочется пожелать Вам их успешного претворения в жизнь.

**Председатель наблюдательного совета Ассоциации защиты информации, член-корреспондент Академии криптографии РФ, действительный государственный советник 3 класса**

**Г. Емельянов**

## ИНЖЕНЕРНАЯ КРИПТОГРАФИЯ

УДК 003.26

# Блочное шифрование в режиме криптокодирования с двумя метками избыточности

*А. А. Костина*; *Н. А. Молдовян*, д-р техн. наук
Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, Россия

*Е. В. Морозова*, канд. техн. наук
АО «НИИ «Вектор», Санкт-Петербург, Россия

*Предложен способ преобразования информации, совмещающий в едином процессе преобразования "шифрование информации" и "помехоустойчивое кодирование". В основе предложенного способа лежит внесение избыточности в преобразуемые данные в виде двух меток, представляющих собой заранее заданные двоичные векторы. Над преобразуемыми блоками данных выполняют блочное шифрующее преобразование. При этом одна метка избыточности встраивается до, а другая — после шифрующего преобразования, за которым следует дополнительное расширяющее криптографическое преобразование. Последнее представляет собой процесс решения системы из двух линейных уравнений с двумя неизвестными, в которых коэффициентами являются подключи. Роль первой метки состоит в снижении вероятности ложного декодирования, а роль второй — в существенном уменьшении числа перебираемых вариантов потенциально возможных ошибок. Благодаря последнему обеспечивается повышение производительности процесса расшифровывания по сравнению с известным способом криптокодирования.*

*Ключевые слова:* блочное шифрование, секретный ключ, метка избыточности, исправление ошибок, кодирование, декодирование, криптокодирование.

Для защиты информации, передаваемой по открытым каналам связи, достаточно широко используют алгоритмы блочного шифрования [1—3]. Блочные шифры (БШ) обладают выраженным свойством размножения ошибок (лавинный эффект), поэтому при передаче блоков шифртекста по каналам с шумом необходимо выполнить дополнительно процедуры помехоустойчивого кодирования. Другими способами применения БШ являются следующие: построение хэш-функций, защита информации в побочных каналах (использование шифрования по известному ключу), гарантированное уничтожение информации на магнитных носителях [4] и построение случайных латинских квадратов большого размера [5]. Сравнительно недавно было предложено использовать БШ для построения алгоритмов криптокодирования, которые совмещают защиту информации от несанкционированного доступа и возможность исправления ошибок, возникающих при передаче шифртекста по каналам с шумом [6]. Предложенный в [6] способ фактически представляет собой использование БШ в режиме исправления ошибок и обладает следующими практическими достоинствами: возможность исправления ошибок при использовании многих известных БШ, например представленных в работах [7, 8]; возможность исправления ошибок различного типа (инверсии, пропуски и вставки битов).

Предложенный способ [6] включает внесение информационной избыточности в шифруемые блоки данных путем присоединения к исходным блокам данных заранее заданной метки, отсутствие которой в расшифрованном блоке данных является индикатором наличия ошибок. При этом исправление ошибок осуществляют переборным путем — проверкой всех потенциально возможных комбинаций одиночных ошибок. Переборный механизм восстановления ошибок обуславливает недостаток способа [6], состоящий в низкой ско-

**Костина Анна Александровна**, научный сотрудник.
E-mail: anna-kostina1805@mail.ru
**Молдовян Николай Андреевич**, профессор, главный научный сотрудник.
E-mail: nmold@mail.ru
**Морозова Елена Владимировна**, ученый секретарь НТС.
E-mail: lenmor@mail.ru

*Статья поступила в редакцию 20 декабря 2019 г.*

рости процесса расшифровывания при наличии нескольких ошибок в блоках шифртекста.

Предлагается новый способ криптокодирования на основе блочных шифрующих преобразований, который применим в наиболее важном для практики случае ошибок, представляющих собой битовые инверсии. Способ включает встраивание двух меток избыточности на разных этапах преобразования входного блока данных. Одна из меток служит в качестве индикатора подмножества возможных комбинаций ошибок, а вторая — в качестве индикатора правильно найденной комбинации. Этот механизм обеспечивает существенное повышение производительности процедуры расшифровывания за счет резкого уменьшения числа перебираемых потенциально возможных комбинаций ошибок.

## Использование блочных шифров в режиме криптокодирования

В режиме блочного шифрования с исправлением ошибок [6] преобразуемый $n$-битовый блок данных формируется путем присоединения к блоку информационных данных $T$ размером $n - \mu$ бит некоторой заданной метки размером $\mu$ бит. При этом исправление ошибок в блоке шифртекста, переданного по каналу с шумом, выполняется путем перебора потенциально возможных комбинаций одиночных битовых ошибок. В принятом блоке шифртекста исправляются предполагаемые ошибки, а затем осуществляется расшифровывание. При наличии в восстановленном блоке метки избыточности принимается решение о том, что ошибки исправлены правильно. Поскольку в процессе исправления ошибок выполняется расшифровывание, его может осуществить только санкционированный получатель, которому известен ключ шифрования. Механизм исправления ошибок [6] является универсальным, что определяется его переборной природой. Универсальность способа [6] заключается в возможности исправления комбинаций одиночных ошибок различного типа, например битовых инверсий, пропусков и вставок битов (включая случай исправления одиночных ошибок различного типа, присутствующих в одном и том же блоке шифртекста).

## Способ криптокодирования с двумя метками избыточности

Пусть задан некоторый алгоритм блочного шифрования $E_K(B)$ с размером входного блока $n = 128$ бит и ключом $K = (K_1, K_2, K_3, K_4)$, где $K_i$ — 64-битовые случайные подключи ($i = 1, 2, 3, 4$). Первая 32-битовая метка избыточности $L_1$ присоединяется к 96-битовому блоку информационных данных $T$, в результате чего формируется 128-битовый входной блок $B = T\|L_1$, который преобразуется в 128-битовый блок шифртекста $C_T = E_K(T\|L_1)$, где $\|$ — операция конкатенации битовых строк. Шифртекст $C_T$ представляется в виде конкатенации 72-битового подблока $C_{T1}$ и 56-битового подблока $C_{T2}$: $C_T = C_{T1}\|C_{T2}$.

Далее к подблоку шифртекста $C_{T2}$ присоединяется 16-битовая метка $L_2$, в результате чего формируется 72-битовый двоичный вектор $C_{T2}\|L_2$, и выполняется вспомогательное шифрующее преобразование расширенного блока шифртекста $C_{T1}\|C_{T2}\|L_2$, заключающееся в решении следующей системы из двух линейных уравнений с двумя 72-битовыми неизвестными $C_1$ и $C_2$:

$$\begin{cases} K_1C_1 \oplus K_2C_2 = C_{T1} \bmod \eta(x); \\ K_3C_1 \oplus K_4C_2 = C_{T2} \,\|\, L_2 \bmod \eta(x), \end{cases} \quad (1)$$

где подключи $K_i$ и подблоки шифртекста $C_{T1}$ и $C_{T2}\|L_2$ рассматриваются как двоичные многочлены, т. е. как элементы конечного поля $GF(2^{72})$;

$\oplus$ — операция сложения двоичных многочленов (XOR);

$\eta(x)$ — неприводимый двоичный многочлен степени 72.

Для того чтобы данная система имела решение, на процедуру генерации ключа шифрования накладывается требование выполнимости соотношения $K_1K_4 \bmod \eta(x) \neq K_3K_2 \bmod \eta(x)$.

Решение системы уравнений (1) дает 144-битовый блок шифртекста $C = C_1\|C_2$. При передаче шифртекста $C$ по каналу с шумом приемная сторона получает блок шифртекста $C'$, содержащий ошибки типа битовых инверсий. Конкретный набор одиночных ошибок характеризуется вектором ошибок

$$\delta = C' \oplus C = (C_1', C_2') \oplus (C_1, C_2) = (\delta_1, \delta_2),$$

где $\delta_1 = C_1' \oplus C_1$; $\delta_2 = C_2' \oplus C_2$.

Подстановка значений $C_1'$ и $C_2'$ в (1) дает следующую систему уравнений:

$$\begin{cases} K_1C_1' \oplus K_2C_2' = C_{T1}' \bmod \eta(x); \\ K_3C_1' \oplus K_4C_2' = C_{T2}' \,\|\, L_2' \bmod \eta(x), \end{cases} \quad (2)$$

в которой в правой части присутствуют неправильно восстановленные значения $C_{T1}$ и $C_{T2}\|L_2$. Получателю неизвестны значения $C_{T1}$ и $C_{T2}$, но известно значение метки $L_2$, поэтому он может вычислить отклонение $\delta_{L2}$ восстановленного значения $L_2'$ от $L_2$. Число возможных 16-битовых зна-

чений $\delta_{L2}$ равно $2^{16}$, и каждому из них соответствует некоторое подмножество значений 128-битовой ошибки $\delta$.

Вычитая из второго уравнения системы (2) второе уравнения системы (1), получаем следующее соотношение:

$$K_3\delta_1 \oplus K_4\delta_2 = \delta_{CT2} \,\|\, \delta_{L2} \bmod \eta(x), \qquad (3)$$

из которого видно, что отклонение $\delta_{L2} = L'_2 \oplus L_2$ восстановленного значения $L'_2$ второй метки от ее правильного значения $L_2$ не зависит от зашифрованного блока информационных данных и от первой метки $L_1$, а зависит только от ключа шифрования. Поэтому, используя уравнение (2), для заданного ключа шифрования $K$ можно вычислить значение отклонения $\delta_{L2}$ для каждого возможного значения вектора ошибок (соответствующих множеству всех комбинаций одиночных ошибок, для которых предполагается обеспечить возможность их исправления). По этим результатам предполагается составить таблицу, указывающую подмножество значений вектора ошибок $\{\delta\}_j$, соответствующее каждому возможному значению отклонения $\delta_{L2} = j$.

**Общий вид таблицы, указывающей подмножество значений вектора ошибок**

| $\delta_{L2} = j =$ | 0 | 1 | 2 | ⋯ | $2^{16}-1$ |
|---|---|---|---|---|---|
| $\{\delta\}_j$ | $\{\delta\}_0$ | $\{\delta\}_1$ | $\{\delta\}_2$ | ⋯ | $\{\delta\}_{2^{16}-1}$ |

Рассмотрим случай, когда требуется обнаружить и восстановить 4 ошибки. Количество 128-битовых векторов ошибок, имеющих вес Хемминга, не превышающий значение 4, равно значению $N$, которое может быть вычислено по формуле $N = \sum_0^4 C_i^{144} < 2^{24}$. В среднем одному значению $\delta_{L2}$ соответствуют $N/2^{16}$ различных значений вектора ошибок, т. е. вычисленное значение $\delta_{L2}$ указывает на подмножество возможных ошибок мощностью, не превышающей числа $2^8$. Таким образом, после вычисления значения $\delta_{L2}$ для исправления ошибок останется выполнить перебор по $2^8$ различным вариантам ошибок. При этом для каждого варианта восстанавливается значение блока шифртекста $C_{T1}\|C_{T2}$ и осуществляется его расшифровывание:

$$B' = E_K^{-1}\left(C_{T1} \,\|\, C_{T2}\right) = T' \,\|\, L'_1,$$

где $E_K^{-1}$ — функция блочного расшифровывания, обратная к $E_K$. Правильному значению восстановленного информационного блока данных $T' = T$ соответствует полученное значение 32-битовой метки $L'_1 = L_1$.

В рассмотренном способе криптокодирования используют предвычисления, в результате которых строится таблица подмножеств значений вектора ошибок, размер которой составляет $\approx 200$ Мбайт для случая исправления 4 ошибок и использования 128-битовой функции блочного шифрования. С уменьшением числа исправляемых ошибок размер таблицы существенно уменьшается. Например, при исправлении 3 ошибок ее размер составляет $\approx 6$ Мбайт. Используемые предвычисления зависят от секретного ключа, разделяемого участниками сеанса защищенной связи, т. е. при смене секретного ключа требуется выполнить вычисление новой таблицы. С учетом этого представляет интерес использование независимых подключей при выполнении блочного шифрования и вспомогательного шифрования, связанного с решением системы уравнений (1). Это позволит выполнить обновление сеансовых ключей в части блочного шифрования, сохраняя подключи вспомогательного шифрования неизменными достаточно долго, благодаря чему устраняется необходимость частого пересчета таблицы разбиения значений вектора ошибки на подмножества.

Рассмотренный способ криптокодирования может быть легко встроен в схемы блочного псевдовероятностного шифрования [9], в которых также используется вспомогательное шифрование в виде процедуры решения системы линейных уравнений.

## Заключение

Предложен способ построения алгоритмов криптокодирования, обеспечивающий повышение производительности процедуры восстановления исходных информационных блоков данных по сравнению с известными алгоритмами-аналогами. В основу способа положена идея включения в процесс криптокодового преобразования дополнительной метки избыточности, служащей в качестве индикатора подмножества возможных значений вектора ошибок.

Представляют интерес реализации предложенного способа при других значениях размера входного блока шифрующей функции $E$ ($n$ = 64, 96) и других соотношениях размеров меток и блока информационных данных.

*Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-57-54002-Вьет_а.*

**Литература**

1. *Bac Do Thi, Minh Hieu Nguyen.* A high speed block cipher algorithm // International J. Security and Its Applications. 2013. V. 7. № 6. P. 43—54.
2. ГОСТ Р 34.12–2015 Информационная технология. Криптографическая защита информации. Блочные шифры. — М.: Стандартинформ, 2015. — 25 с.
3. ГОСТ Р 34.13–2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. — М.: Стандартинформ, 2015. — 42 с.
4. *Мирин А. Ю.* Метод и алгоритм гарантированного уничтожения информации, хранимой на магнитных дисках: автореф. дис. канд. тех. наук. — СПб., 2005. — 20 с.
5. *Молдовян Н. А., Нгуен Ле Минь, Хо Нок Зуй.* Синтез поточных шифров на основе блочных преобразований: метод латинских квадратов // Вопросы защиты информации. 2008. № 1. С. 27—34.
6. *Moldovyan N., Levina A., Taranov S.* Symmetric Encryption for Error Correction: Proceedings of the 20th FRUCT'20 Conference. 3—7 April 2017. — SPb: Saint-Petersburg Electrotechnical University "LETI" and Technopark of ITMO University. P. 290—295. DOI: 10.23919/FRUCT.2017.8071325.
7. *Moldovyan N. A., Moldovyan A. A.* Data-driven block ciphers for fast telecommunication systems. — New York, London. Auerbach Publications. Talor & Francis Group. 2008. — 185 p.
8. *Pieprzyk J., Hardjono Th., Seberry J.* Fundumentals of Computer Security. — Berlin: Springer-verlag, 2003. — 677 p.
9. *Морозова Е. В., Мондикова Я. А., Молдовян Н. А.* Способы отрицаемого шифрования с разделяемым ключом // Информационно-управляющие системы. 2013. № 6. С. 73—78.

# Block encryption in the error-correcting mode with two redundancy labels

*A. A. Kostina, N. A. Moldovyan*
St. Petersburg Institute for Informatics and Automation the RAS, St. Petersburg, Russia

*E. V. Morozova*
Scientific Research Institute "Vektor", St. Petersburg, Russia

*There is proposed a method for information transformation including in a single process of the data transformation both the block encryption and the error correction. The proposed method is based on insetting the redundancy in the form of two labels that are preliminary fixed and represent binary vectors. The transformed data are encrypted using a block cipher. One of the redundancy labels is imbedded before the encryption process. The second one is imbedded after the encryption procedure followed by the additional cryptographic transformation that extends the transformed data block. The additional cryptographic transformation represents a process of solving a system of two linear equations with two unknowns, in which the subkeys are used as coefficients of the linear equations. The first redundancy label is used to reduce the probability of false decoding. The second label is used to reduce significantly the number of the potentially possible combinations of the errors. Due to the last the performance of the decryption procedure is essentially higher than in the known methods for error-correcting ciphering.*

*Keywords*: block encryption, secret key, redundancy label, error correcting, encoding, decoding, ciphering, cryptocoding.

Bibliography — 9 references. *December 20, 2019*

УДК 621.372.552

# Двухкомпонентная стеганографическая система на основе суммы линейных функций двух сигналов, использующая аддитивный вид связи встраиваемых сигналов

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

*Рассматривается стеганографическая двухкомпонентная система на основе суммы линейных функций двух сигналов, инвариантная к маскирующему сигналу, и определяется ключевой коэффициент, позволяющий обеспечить эффективную защиту скрытого сигнала от несанкционированного восстановления.*

*Ключевые слова:* двухкомпонентная стеганографическая система, инвариантность к маскирующему сигналу, стеганографический контейнер, ключевой коэффициент.

Двухкомпонентная стеганографическая система [1—10] позволяет заменить с помощью маскирующего сигнала значение отсчета скрываемой информации парой значений из множества возможных. Если значения в паре связаны известным образом, то скрываемое значение может быть восстановлено. Кроме того, функции алгоритмов восстановления имеют разрывы, что позволяет получить высокую чувствительность алгоритмов к вариации некоторых коэффициентов. Такие коэффициенты по аналогии с криптографическими системами будем считать ключевыми коэффициентами.

В работе [1] рассматривается двухкомпонентная стеганографическая система на основе произведения линейных функций двух сигналов. Особенностью системы является нелинейность преобразования скрываемого значения в пару значений контейнера [7]. Частным случаем такой системы является система на основе суммы линейных функций двух сигналов, сохраняющая линейность преобразования и разрывы в алгоритме восстановления. Сумма линейных функций двух сигналов имеет следующий вид:

$$y = (a_1 + b_1 u_1) + (a_2 + b_2 u_2). \tag{1}$$

Выражение (1) преобразуется к виду

$$y = a + bu_1 + cu_2, \tag{2}$$

где $a$, $b$ и $c$ — коэффициенты.

Распространяя (2) на две компоненты контейнера, получим

$$\begin{cases} y_1 = a_1 + b_1 u_1 + c_1 \xi; \\ y_2 = a_2 + b_2 u_2 + c_2 \xi, \end{cases} \tag{3}$$

где $u_1$ и $u_2$ — информативные сигналы, полученные из скрываемого информативного сигнала $u$;

$\xi$ — маскирующий сигнал (сигнал контейнера).

Рассмотрим аддитивный вид связи встраиваемых сигналов:

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

Решим систему (3), выразив из второго уравнения $\xi$:

$$\xi = \frac{y_2 - a_2 - b_2 u_2}{c_2}. \tag{5}$$

Подставим (5) в первое уравнение (3) и получим

$$y_1 = a_1 + b_1 u_1 + c_1 \frac{y_2 - a_2 - b_2 u_2}{c_2}. \tag{6}$$

Преобразуем (6) относительно $u_1$, используя (4):

$$u_1 b_1 c_2 - u_2 b_2 c_1 + a_1 c_2 - a_2 c_1 + c_1 y_2 - c_2 y_1 = 0; \tag{7}$$

$$\begin{aligned} u_1 (b_1 c_2 + b_2 c_1) + K b_2 c_1 + a_1 c_2 - a_2 c_1 + \\ + c_1 y_2 - c_2 y_1 = 0. \end{aligned} \tag{8}$$

Решение (8) позволяет восстановить скрываемое значение:

$$u = u_1 = \frac{K b_2 c_1 - a_1 c_2 + a_2 c_1 - c_1 y_2 + c_2 y_1}{b_1 c_2 + b_2 c_1}. \tag{9}$$

Таким образом, (9) является алгоритмом восстановления скрытого сигнала.

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

*Статья поступила в редакцию 30 января 2020 г.*

## Исследование

Получим выражения для чувствительности (9) к вариации коэффициентов. Для этого определим дифференциал $u_1$ через приращения коэффициентов.

Количество коэффициентов в (9) равно шести. Помимо этого используется значение $K$. Выражение для абсолютной чувствительности алгоритма восстановления ищем в виде

$$\Delta_{u_1} = S_{a_1}\Delta_{a_1} + S_{a_2}\Delta_{a_2} + S_{b_1}\Delta_{b_1} + S_{b_2}\Delta_{b_2} + \\ + S_{c_1}\Delta_{c_1} + S_{c_2}\Delta_{c_2} + S_K\Delta_K. \quad (10)$$

Получим необходимые производные для перехода к приращениям в выражении (10). Очевидно, что максимум чувствительности (9) к вариации коэффициентов будет вблизи точки разрыва. Данная область определяется выражением

$$b_1c_2 + b_2c_1 = \sigma \text{ при } \sigma \to 0, \quad (11)$$

где $\sigma$ — величина отклонения от точки разрыва.

Знаменатель выражения (9) не содержит принимаемые сигналы $y_1$ и $y_2$, поэтому рабочая точка алгоритма восстановления фиксирована. Очевидно, что чем меньше значение $\sigma$, чем ближе рабочая точка алгоритма к точке разрыва, тем выше чувствительность алгоритма восстановления к вариации коэффициентов.

Найдем выражения коэффициентов чувствительности $S$ в (10). Для этого используем производные по всем коэффициентам:

$$S_{a_1} = \frac{du_1}{da_1} = -\frac{c_2}{b_1c_2 + b_2c_1}; \quad (12)$$

$$S_{a_2} = \frac{du_1}{da_2} = \frac{c_1}{b_1c_2 + b_2c_1}; \quad (13)$$

$$S_{b_1} = \frac{du_1}{db_1} = \frac{c_2\left(-a_1c_2 + a_2c_1 - c_1y_2 + c_2y_1 + Kb_2c_1\right)}{\left(b_1c_2 + b_2c_1\right)^2}; \quad (14)$$

$$S_{b_2} = \frac{du_1}{db_2} = \frac{c_1\left(a_1c_2 - a_2c_1 + c_1y_2 - c_2y_1 + Kb_1c_2\right)}{\left(b_1c_2 + b_2c_1\right)^2}; \quad (15)$$

$$S_{c_1} = \frac{du_1}{dc_1} = \frac{c_2\left(a_1b_2 + a_2b_1 - b_1y_2 - b_2y_1 + Kb_1b_2\right)}{\left(b_1c_2 + b_2c_1\right)^2}; \quad (16)$$

$$S_{c_2} = \frac{du_1}{dc_2} = -\frac{c_1\left(a_1b_2 + a_2b_1 - b_1y_2 - b_2y_1 + Kb_1b_2\right)}{\left(b_1c_2 + b_2c_1\right)^2}; \quad (17)$$

$$S_K = \frac{du_1}{dK} = \frac{b_2c_1}{b_1c_2 + b_2c_1}. \quad (18)$$

Значения $y_1$ и $y_2$ содержат в себе значения всех коэффициентов, однако принимающая сторона получает их в виде текущих констант. При дифференцировании $y_1$ и $y_2$ не раскрываются.

Выражения (12), (13) и (18) не зависят от соответствующих варьируемых коэффициентов, поэтому погрешность восстановления представляет собой линейную функцию варьируемого коэффициента.

Выражения (14)—(17) — гиперболические зависимости соответствующих варьируемых коэффициентов, поэтому погрешность восстановления будет иметь разрыв.

Зная коэффициенты преобразования (3) с помощью выражений (12)—(18) можно оценить чувствительность системы к вариации того или иного коэффициента и выбрать коэффициент наиболее подходящий на роль ключевого коэффициента, который является секретным. Для наглядности определения, какой из коэффициентов наиболее эффективно использовать в качестве ключевого, определим характер искажения восстановленного полезного сигнала при внесении ошибки в тот или иной коэффициент. Для этого воспользуемся численным моделированием. Зададим исходные значения:

$$a_1 = 0{,}1;\ a_2 = 0{,}3;\ b_1 = -2{,}1;\ b_2 = 1{,}7;$$

$$c_1 = 3;\ K = 0{,}2;\ \sigma = 1\cdot10^{-9}.$$

С помощью (11) найдем $c_2$:

$$c_2 = \frac{\sigma - b_2c_1}{b_1} = 2{,}429.$$

Формируя случайный информационный и маскирующий сигнал, реализуем стеганографическую систему в соответствии с (3) и при восстановлении полезного сигнала с помощью (9) внесем ошибку в соответствующие коэффициенты. На рис. 1 приведена зависимость маскирующего сигнала $\xi$ и сигналов передаваемых компонент $y_1$ и $y_2$. Видно, что форма сигналов компонент сходна с формой маскирующего сигнала. При заданных параметрах системы коэффициенты корреляции компонент и полезного сигнала равны 0,22, что говорит о достаточно эффективном сокрытии сигнала. При внесении в значения коэффициентов ошибки, равной $\delta = 1\cdot10^{-10}$, получена зависимость, приведенная далее. Заметим, что характер зависимости при внесении ошибки в коэффициенты первой и второй компонент сходен. Поэтому на рисунках представлена только зависимость, полученная при внесении ошибки в коэффициенты первой компоненты.

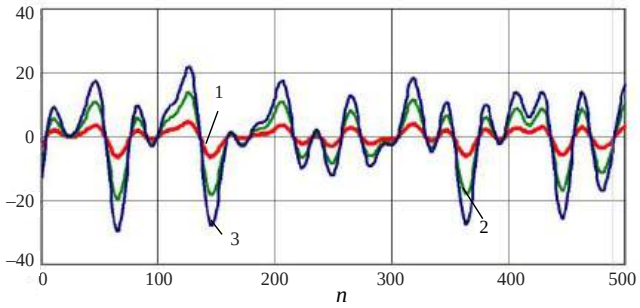



***Рис. 1. Сигнал пустого и двух компонент заполненного контейнера:***
$1 — \xi_n$ ; $2 — y_{1n}$ ; $3 — y_{2n}$

На рис. 2 приведены графики исходного и восстановленного сигналов при внесении ошибки в коэффициент $a_1$. Видно, что в этом случае появляется постоянная составляющая, которая легко исключается из сигнала. Следовательно, использование в качестве ключевых коэффициентов $a$ в данном алгоритме восстановления исключается. Аналогичный результат получен и при внесении ошибки в коэффициент $K$.

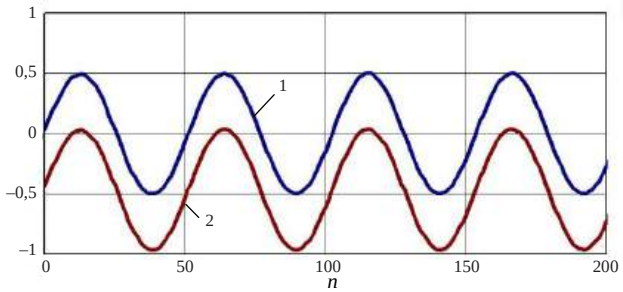



***Рис. 2. Исходный и декодированный информационные сигналы при ошибке в коэффициенте $a_1$:***
$1 — u_{1\text{ис}n}$ ; $2 — u_{1\text{вос}n}$

На рис. 3 приведены графики исходного и восстановленного сигналов при внесении ошибки в коэффициент $b_1$. Видно, что в этом случае изменяется амплитуда восстановленного сигнала, что легко корректируется. Следовательно, использование в качестве ключевых коэффициентов $b$ в данном алгоритме восстановления также исключается.

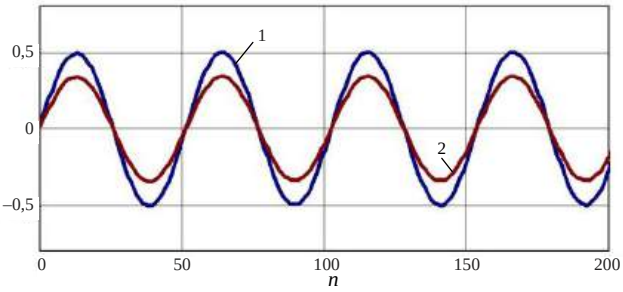



***Рис. 3. Исходный и декодированный информационные сигналы при ошибке в коэффициенте $b_1$:***
$1 — u_{1\text{ис}n}$ ; $2 — u_{1\text{вос}n}$

На рис. 4 приведены графики исходного и восстановленного сигналов при внесении погрешности в коэффициент $c_1$. Видно, что в этом случае информативный сигнал маскируется случайным сигналом, что говорит об эффективности использования в качестве ключевых коэффициентов $c$.

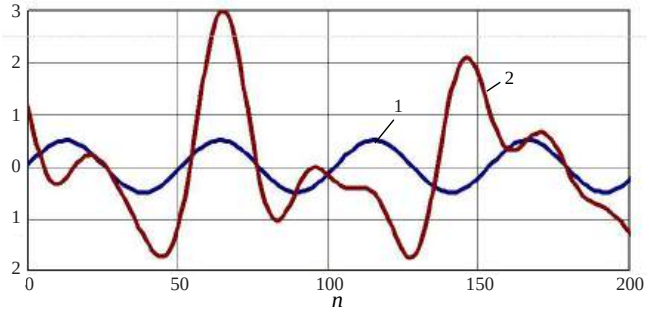



***Рис. 4. Исходный и декодированный информационные сигналы при ошибке в коэффициенте $c_1$:***
$1 — u_{1\text{ис}n}$ ; $2 — u_{1\text{вос}n}$

Рассмотрим влияние изменения ошибки значения коэффициента $c$ на спектр восстановленного сигнала. На рис. 5 приведена поверхность, показывающая изменение спектра восстановленного сигнала от ошибки $\delta \cdot 10^{-11}$ в значении коэффициента $c_1$ от изменения $\delta$. Видно, что при нулевой ошибке спектр состоит из одной гармоники. При увеличении ошибки гармоника информативного сигнала скрывается в спектре маскирующего сигнала.

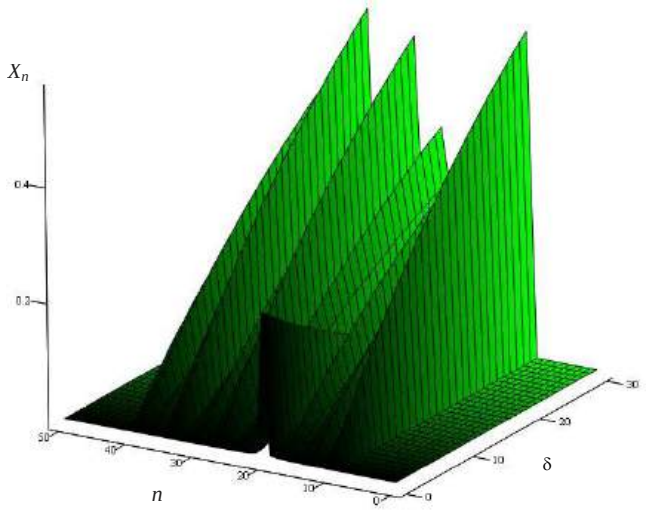



***Рис. 5. Зависимость спектра восстановленного сигнала от ошибки, внесенной в коэффициент $c_1$***

Отметим, что при значении $\sigma = 1 \cdot 10^{-9}$ и при ошибке значения $c_1$ $20 \cdot 10^{-11}$ гармоника информативного сигнала полностью скрывается в спектре маскирующего сигнала.

## Заключение

В результате проведенного исследования получен важный результат, показывающий, что при синтезе двухкомпонентной инвариантной стеганографической системы на основе суммы линейных функций двух сигналов, использующей аддитивную связь встраиваемых в компоненты сигналов, в качестве ключевого коэффициента необходимо использовать только коэффициенты *c*. Использование других коэффициентов не приводит к маскировке информативного сигнала при ошибочном подборе коэффициентов алгоритмов восстановления.

**Литература**


1. *Шакурский М. В.* Математические модели двухкомпонентных инвариантных стеганографических систем, использующих различные алгоритмы связи встраиваемых сигналов // Вопросы защиты информации. 2018. № 2 (121). С. 8—13.

2. *Шакурский М. В., Шакурский В. К.* Устройство сокрытия информации. Патент 2546307 РФ, МПК H04L 9/00, H04K 3/00. Заявл. 10.06.2014. Опубл. 10.04.2015. Бюл. 10.

3. *Шакурский М. В., Шакурский В. К.* Способ скрытой передачи информации. Патент 2546306 РФ, МПК H04L 9/00, H04K 3/00. Заявл. 10.06.2014. Опубл. 10.04.2015. Бюл. 10.

4. *Шакурский М. В.* Устройство сокрытия информации. Патент 167074 РФ, МПК H04L 9/00, H04K 3/00. Заявл. 28.01.2016. Опубл. 20.12.2016. Бюл. № 35.

5. *Шакурский В. К., Шакурский М. В., Козловский В. Н., Сорокин А. Г.* Устройство сокрытия информации. Патент 174362 РФ, МПК H04L 9/00, H04K 3/00, G06F 21/00. Заявл. 23.03.2017. Опубл. 11.10.2017. Бюл. № 29.

6. *Шакурский В. К., Шакурский М. В.* Сжимающие отображения в инвариантных преобразователях и системах стеганографии. — Самара: Изд-во СНЦ РАН, 2014.

7. *Шакурский М. В.* Формирование контейнера для стеганографической системы на основе сжимающих отображений // Радиотехника. 2015. № 2. С. 134—139.

8. *Шакурский М. В., Шакурский В. К.* Стеганографическая система на основе сжимающих отображений // Вопросы защиты информации. 2015. № 2. С. 74—78.

9. *Шакурский М. В., Шакурский В. К.* Оценка стойкости двухкомпонентной стеганографической системы // Успехи современной радиоэлектроники. 2015. № 11. С. 87—91.

10. *Шакурский М. В., Шакурский В. К.* Двухканальная система сокрытия информации с взаимным зашумлением каналов // Радиотехника. 2016. № 2. С. 96—99.


# Two-component steganographic system based on sum of linear functions of two signals with additive constraint of embedded signals


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



*The article considers a steganographic two-component system based on the sum of the linear functions of two signals, which is invariant to a masking signal, and determines a key coefficient that allows effective protection of embedded signal from unauthorized extraction.*



*Keywords:* two-component steganographic system, invariance to masking signal, steganographic container, key coefficient.

Bibliography — 10 references *Received January 30, 2020*

# УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004.056.55

## Механизм аутентификации в системах связи БПЛА

*К. В. Борисов*; *И. Е. Любушкина*, канд. техн. наук; *С. П. Панасенко*, канд. техн. наук
ООО Фирма «АНКАД», Москва, Россия

*Представлен один из способов адаптации существующих решений взаимной аутентификации участников информационного обмена под ограниченные аппаратные и программные ресурсы беспилотных летательных аппаратов (БПЛА) и под низкую пропускную способность каналов управления ими. Реализованы выработка и распределение сеансовых ключей шифрования и расчета имитовставки, которые в дальнейшем используются для защиты сообщений в канале управления. Реализована процедура шифрования передаваемых сообщений с защитой от навязывания ранее переданных сообщений. На основании представленных методов защиты предполагается реализация стойкой системы защиты информации, циркулирующей в каналах управления беспилотных авиационных систем (БАС) в условиях ограниченной ресурсоемкости летательных аппаратов.*

*Ключевые слова:* протокол Диффи—Хеллмана, аутентификация, БПЛА, асимметричные ключи.

### Проблема защиты канала управления беспилотными летательными аппаратами

Вопрос защиты информации в БАС различного назначения стоит достаточно остро. Весь информационный поток, циркулирующий в типичной БАС, можно условно разделить на информацию управления и пользовательскую целевую информацию.

В большинстве случаев БАС включает два типа объектов: наземные станции управления (НСУ) и БПЛА. В зависимости от размера БАС в ней может присутствовать несколько НСУ. НСУ либо управляет своей подчиненной группой БПЛА, либо играет роль резервных систем. Количество БПЛА, как правило, не ограничено. Их привязка к конкретной НСУ зависит от топологии системы.

Основной информационный обмен происходит между НСУ и подчиненным ей БПЛА. В системе БПЛА типа "рой" функции НСУ делегируются одному из БПЛА, который управляет группой летательных аппаратов. НСУ генерирует поток управляющей информации, в то время как БПЛА генерирует ответы на управляющие воздействия и целевую информацию. Целевая информация может либо передаваться на НСУ, либо записываться на информационные носители в конструкции БПЛА.

Управляющая и целевая информация может передаваться по одному радиоканалу либо по отдельным радиоканалам. Рассмотрим случай, когда управляющая информация передается по выделенному каналу управления (КУ). Управление БПЛА может осуществляться полностью ручным, полуавтоматическим и автоматическим способом. В зависимости от типа управления производится периодический или постоянный обмен данными между БПЛА и НСУ: команды ручного управления, координаты целеназначения, телеметрическая информация, информация от устройств полезной нагрузки. В большинстве случаев КУ БАС имеют низкую пропускную способность, команды управления просты и коротки, а протоколы управления максимально упрощены с целью добиться оперативного отклика БПЛА на команды управления.

Ввиду доступности радиоэфира нарушителю каналы управления подвержены множеству атак, проводимых удаленно, без физического контакта с оборудованием.

Существуют две категории атак.

- Радиоэлектронное подавление (все виды атак, направленных на подавление канала связи или навигационного оборудования БПЛА);
- Информационные атаки (атаки, целью которых являются изучение информационного содержания радиообмена и последующая имитация вы-

**Борисов Кирилл Викторович**, старший инженер.
E-mail: kb@ancud.ru
**Любушкина Ирина Евгеньевна**, главный специалист.
E-mail: il@ancud.ru
**Панасенко Сергей Петрович**, заместитель генерального директора.
E-mail: sp@ancud.ru

*Статья поступила в редакцию 25 декабря 2019 г.*

деленных команд; основные типы атак этой категории: DoS, MitM, Replay, Spoofing).

В данной работе рассматривается способ защиты КУ БАС методами криптографической защиты. Описанный способ защиты способен предотвратить лишь информационные атаки. Он включает аутентификацию участников информационного обмена, аутентификацию и конфиденциальность всех сообщений в КУ БАС, а также систему ключевого распределения между участниками.

### Синтез решений информационной защиты в канале управления

В основу разработанных методов защиты легли известные алгоритмы и протоколы. Основная работа проведена в области адаптации выбранных алгоритмов и протоколов под ограниченные аппаратные и программные ресурсы БПЛА и под низкую пропускную способность канала управления. Цель — реализовать легковесную, но криптографически стойкую систему защиты канала управления на симметричных алгоритмах шифрования. При этом разработанные решения не должны существенно усложнять процесс обмена данными в реальном масштабе времени, нарушать оперативность передачи команд.

Реализация функций защиты была выполнена в отдельном криптографическом модуле. В БПЛА модуль имеет исполнение отдельной аппаратной платформы, которая включается в разрыв между полетным контроллером и трансивером. В НСУ модуль представляет собой программное приложение.

При выборе алгоритмов аутентификации учитывались следующие моменты. Большинство известных протоколов аутентификации базируется на использовании клиент-серверной технологии и ориентировано на применение в больших сетях с наличием нескольких клиентов. При этом для правильного функционирования большинства протоколов должен быть реализован отдельный сервер аутентификации или сертифицирующий центр, выдающий и авторизующий ключи пользователей или сертификаты. При реализации в БАС использование таких систем избыточно и нецелесообразно.

Еще одной краеугольной задачей стала разработка системы ключевого распределения. Был выбран вариант предполетной подготовки с записью сеансовых ключей в криптографические модули. В качестве ключевых носителей были выбраны внешние устройства типа смарт-карт или токенов. При этом инициатором работы с внешними ключевыми носителями должен быть непосредственно криптографический модуль (программный или аппаратный), расположенный на БПЛА и НСУ. Для полноценной реализации предполагаемого способа защиты ключевые носители должны иметь в наличии:

- собственные вычислительные ресурсы;
- операционную систему и/или управляющее микропрограммное обеспечение;
- собственную оперативную и энергонезависимую память с защищенной областью данных;
- встроенные криптографические функции.

В качестве ключевых носителей могут быть использованы смарт-карты с контактным или бесконтактным интерфейсом, соответствующие семействам стандартов ГОСТ Р ИСО/МЭК 7816 и/или ГОСТ Р ИСО/МЭК 14443. В качестве альтернативного варианта ключевого носителя могут быть использованы криптографические токены, подключаемые к порту USB и имеющие систему команд, аналогичную описанной в стандартах ГОСТ Р ИСО/МЭК 7816-4 и ГОСТ Р ИСО/МЭК 7816-8.

Работа с ключевыми носителями осуществляется при наличии программно-аппаратных интерфейсов, предназначенных для ввода ключей. При этом интерфейсы могут быть съемными, так как в предполагаемом способе они не требуют постоянного подключения и реализуются только при предполетной подготовке и первоначальном установлении соединения, после чего могут быть отключены.

Начальное распределение ключей осуществляется по протоколу Диффи—Хеллмана на эллиптических кривых. В соответствии с данным протоколом у обоих участников обмена должны быть личный секретный ключ и личный открытый ключ. Открытые ключи предназначены для обмена по каналам связи для формирования сеансовых ключей индивидуальной парно-выборочной связи.

Для уменьшения вероятности проведения атаки MitM, возможной при обмене открытыми ключами по протоколу Диффи—Хеллмана, введено требование, в соответствии с которым обе стороны должны заранее иметь открытые ключи друг друга. Во время обмена открытыми ключами по протоколу обе стороны сравнивают полученный открытый ключ с имеющимся. При совпадении ключей стороны считают, что обмен ведется с легальным пользователем, а не с несанкционированной третьей стороной.

Таким образом, начальная информация, хранящаяся на ключевом носителе (смарт-карте), должна включать:

- собственный секретный ключ (32 байта);
- собственный открытый ключ (64 байта);

- открытые ключи всех абонентов, с которыми необходимо организовать защищенную связь ($N \cdot 64$ байта).

Для генерации пары секретный ключ—открытый ключ используется команда GENERATE KEY PAIR согласно ГОСТ Р ИСО/МЭК 7816-4. С помощью данной команды генерируется пара ключей в соответствии с алгоритмом ГОСТ Р 34.10-2001. Формируются секретный ключ размером 32 байта и открытый ключ размером 64 байта. Открытый и секретный ключи сохраняются во внутренней энергонезависимой памяти смарт-карты.

### Адаптированный протокол аутентификации в канале управления

Цель протокола аутентификации — установить начальное соединение между НСУ и БПЛА. При этом происходят выработка и распределение сеансовых ключей шифрования и расчета имитовставки, которые в дальнейшем используют для защиты сообщений в канале управления. НСУ должна создать начальное соединение с каждым подчиненным ей БПЛА.

Протокол аутентификации при установлении соединения и выработке сеансовых ключей основан на работе протокола TLS (Transport Layer Security) и является его аналогом, адаптированным под использование в инфраструктуре БПЛА.

Процесс аутентификации и формирования сеансовых ключей разделен на три этапа.

1. Обмен открытыми ключами и проведение двухсторонней аутентификации;
2. Создание общего секретного премастер-ключа на основании собственного секретного ключа и открытого ключа второго участника обмена в соответствии с алгоритмом Диффи—Хеллмана на эллиптических кривых;
3. Создание сеансовых ключей.

Последовательность действий при реализации данного способа представлена следующим образом:

- Криптографический модуль БПЛА (инициатор информационного обмена) отправляет на свою смарт-карту команду GENERAL AUTHENTICATE стандарта ГОСТ Р ИСО/МЭК 7816-4, в результате чего программное обеспечение смарт-карты генерирует общий секретный премастер-ключ. Криптографический модуль БПЛА считывает со смарт-карты свой открытый ключ *Kpublic_uav*, открытый ключ НСУ *Kpublic_gbc* и общий секретный премастер-ключ *Kpre-master*.
- Аналогичные действия производятся на стороне НСУ, в результате чего криптографический модуль НСУ считывает со смарт-карты свой открытый ключ *Kpublic_gbc*, открытый ключ БПЛА *Kpublic_uav* и общий секретный премастер-ключ *Kpre-master*.
- Если операция прошла успешно, то криптографический модуль БПЛА инициирует передачу сообщения криптографическому модулю НСУ. Сообщение *M* (*Kpublic_uav*, *RANDuav*) содержит открытый ключ БПЛА *Kpublic_uav* и выработанное криптографическим модулем БПЛА случайное число *RANDuav*.
- Криптографический модуль НСУ получает сообщение *M* от криптографического модуля БПЛА и проверяет, есть ли у него ключ *Kpublic_uav*. При его наличии в памяти смарт-карты криптографический модуль считает, что сообщение пришло от истинного БПЛА, и аналогичным образом формирует ответное сообщение *M*' (*Kpublic_gbc*, *RANDgbc*).
- Криптографический модуль БПЛА получает сообщение от криптографического модуля НСУ и проверяет, есть ли у него полученный открытый ключ от НСУ. При его наличии БПЛА считает, что получил сообщение от истинного НСУ и приступает к формированию мастер-ключа.
- Криптографические модули на основе общего сеансового премастер-ключа *Kpre-master* и случайных чисел *RANDuav* и *RANDgbc* параллельно вырабатывают мастер-ключ *Kmaster*. Ключ *Kmaster* вырабатывается на основе алгоритма хэширования (например, ГОСТ Р 34.11-2012) или алгоритма вычисления кода аутентификации сообщений на основе алгоритмов хэширования (например, HMAC_GOSTR3411_2012_256). Для формирования мастер-ключа используется режим VKO [1]. Отметим, что премастер-ключ является долговременным, поскольку он основан на долговременных ключах НСУ и БПЛА, тогда как мастер-ключ является сеансовым, поскольку в его генерации участвуют случайные числа БПЛА и НСУ, вырабатываемые, соответственно, на предыдущих шагах описанного алгоритма.
- На основе ключа *Kmaster* в обоих криптографических модулях формируются сеансовый ключ шифрования *Kenc* и сеансовый ключ выработки имитовставки *Kmac*. Формирование сеансовых криптографических ключей осуществляется на основе алгоритма ГОСТ Р 34.13-2015 в режиме выработки имитовставки. Генерация сеансовых ключей на основе мастер-ключа может быть выполнена иными способами. В частности, для этого могут быть использованы любой из алгоритмов шифрования, описанных в стандарте ГОСТ Р 34.12-2015, или функция диверсификации ключей KDF_GOSTR3411_2012_256 [2]. В блоке обеспечения конфиденциальности криптографиче-

ского модуля БПЛА присутствует счетчик пакетов. Каждый криптографический модуль ведет счетчик отправленных и счетчик принятых пакетов. Каждому отправленному пакету присваивается свой порядковый номер. Номер очередного пакета на 1 больше предыдущего. Нумерация пакетов в каждом направлении: 0, 1, 2, 3, 4, …, *N*. Номер каждого принятого пакета считывается и фиксируется. Приему и расшифровке подлежат только пакеты с порядковым номером больше, чем предыдущий принятый. Для каждого пакета формируются свой сеансовый ключ шифрования и свой сеансовый ключ расчета имитовставки, которые обновляются в зависимости от номера пакета. Таким образом, пакеты с одинаковым содержанием, но с разными порядковыми номерами защищаются разными криптографическими ключами, что приводит к качественной рандомизации данных, попадающих в радиоканал.

- Криптографический модуль БПЛА формирует сообщение-ответ, зашифрованное на выработанном сеансовом ключе шифрования *Kenc*, снабжает его имитовставкой, рассчитанной на ключе *Kmac*, и отправляет сообщение-ответ в канал связи, после чего переходит в режим ожидания ответа от криптографического модуля НСУ.
- Криптографический модуль НСУ получает сообщение-ответ от криптографического модуля БПЛА, расшифровывает его и проверяет его имитовставку. Если имитовставка полученного сообщения совпадает с присланной, то криптографический модуль НСУ считает, что сеансовые криптографические ключи установлены верно, формирует аналогичным образом свой ответ и отправляет его в канал связи.
- Криптографический модуль БПЛА получает сообщение-ответ от криптографического модуля НСУ, аналогичным образом расшифровывает его и проверяет его целостность с помощью имитовставки. Если целостность сообщения не нарушена, то криптографический модуль БПЛА считает, что сеансовые криптографические ключи установлены верно.

Сформированные сеансовые ключи хранятся в оперативной памяти до момента перезагрузки. При следующем включении питания процедура установки безопасного соединения и выработки сеансовых ключей повторяется.

## Выводы

Выработанный алгоритм позволяет реализовать безопасную аутентификацию участников информационного обмена, сопровождающуюся распределением ключевой информации. Использование ключевых носителей позволяет сохранять в секрете закрытые ключи БПЛА и НСУ, защищая их от компрометации при утере БПЛА. Извлеченные сеансовые ключи теоретически могут быть использованы только для расшифровки текущего сеанса обмена информацией и не позволяют получать доступ к предшествующему или дальнейшему информационному обмену.

С учетом применения сеансовых ключей, на основании которых формируются ключи шифрования и выработки имитовставки, а также изменение ключей в зависимости от номера пакета, извлечение мастер-ключа является достаточно сложной задачей. В рамках непродолжительности среднего полета БПЛА задача и вовсе является нецелесообразной. Использование внешних ключевых носителей, отключаемых после установки соединения и загрузки ключей, позволяет минимизировать увеличение веса БПЛА и потребление энергии аккумулятора.

В дополнение ко всем заявленным особенностям методов защиты канала управления БАС возможно внедрение в работу парсера протокола управления, а также модуля цифровой подписи шифрованных сообщений для реализации дополнительной защиты от DoS-атак методом фильтрации и недопуска к обработке неподтвержденных или неопознанных пакетов данных. Внедрение функции динамического изменения ключей шифрования и выработки имитовставки позволяет максимально рандомизировать поток данных, находящихся в радиоэфире, усложняя идентификацию пакетов данных и понимание структуры формирования пакетов. Помимо этого разработанные методы усложняют сбор шифрованных данных для сопоставления с известными открытыми данными, так как каждый пакет шифруется своим ключевым набором.

**Литература**

1. *Popov V., Kurepkin I., Leontiev S.* RFC 4357: Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms [Электронный ресурс]. Режим доступа: http://tools.ietf.org/html/rfc4357 — January 2006 — CRYPTO-PRO.

2. Рекомендации по стандартизации Р 50.1.113-2016. Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования.

# Authentication mechanism for UAV communication systems

K. V. Borisov, I. E. Lubushkina, S. P. Panasenko
ANCUD Ltd., Moscow, Russia

*This article considers one of the ways to adapt existing solutions for mutual authentication of information exchange participants for the limited UAV hardware and software resources and for the low bandwidth of the control channel. It presents a method for generation and distribution of encryption and MAC calculation session keys for the subsequent use to protect messages in the control channel. It also describes a mechanism for the protection against the reuse of previously transmitted messages. The described methods can be used to implement a sufficient information protection subsystem with limited resource consumption for UAS control channels.*

*Keywords:* Diffie—Hellman protocol, authentication, UAV, asymmetric keys.

Bibliography — 2 references. *Received 25 December, 2019*

УДК 004:51-7: 519.6

# Управление информационным контуром вуза и его защита с помощью биометрической идентификации: некоторые методы и средства

*К. В. Пителинский*, канд. техн. наук; *Н. В. Федоров*, канд. техн. наук;
*А. И. Чайчиц*; *О. А. Широкова*
ФГБОУ ВО "Московский политехнический университет", Москва, Россия

*Обсуждается необходимость оптимизации и защиты контурных потоков, циркулирующих в вузе, посредством использования в автоматизированной системе управления вузом подсистемы биометрической идентификации персонала и студентов (в частности, для снижения утечек информации). Рассмотрены существующие методы и средства биометрической идентификации.*

*Ключевые слова:* информационная безопасность, управление вузом, биометрия, динамические контурные потоки, СКУД, имитационное моделирование, "золотое сечение".

Интенсификацию применения средств информатизации и информационных технологий (ИТ) в образовательной сфере можно объяснить наметившимся в глобальном масштабе переходом к цифровой экономике, затронувшим все сферы человеческой деятельности. Цифровизация общества движется в сторону интеллектуальных автоматизированных систем управления (АСУ), а вуз является лишь частным примером практического приложения данной тенденции.

При построении АСУ вуза требуется, чтобы она могла анализировать и корректировать в режиме реального времени состояние других систем вуза, а также учитывать влияние на ее функционирование различных событий. Конечным этапом, к которому стремятся разработчики любых АСУ, является создание системы искусственного интеллекта, интегрированного в деятельность предприятий (организаций). В вузах необходимо и достаточно внедрить систему сбора и анализа данных на уровне подразделений, которая хотя и не сможет принимать полностью самостоятельные управленческие решения, но сможет работать по вполне определенным (заложенным ее разработчиками) сценариям, что позволит более качественно организовать процесс управления вузом и вести контроллинг его деятельности в различных разрезах.

Существует много средств, позволяющих идентифицировать личность человека, — это устройства с вводом ПИН-кода, считыватели контактных и бесконтактных смарт-карт, считыватели штрихкодов или QR-кодов, биометрические считыватели и т. п. Более надежными являются биометрические считыватели, так как подделать карточку или взломать ПИН-код гораздо проще, чем украсть биометрический материал конкретного человека.

В вузах государственного образца используют в основном системы, использующие смарт-карты и турникеты, объединенные в систему контроля и управления доступом. Однако смарт-карту легко потерять, а за пропуск через турникет отвечают люди. Рассмотрим основные методы биометрической идентификации пользователей информационных систем (ИС), обеспечивающих заслон от проникновения злоумышленника на объект информатизации, в рассматриваемом случае это территория вуза.

Согласно данным ресурса Infowatch, с каждым годом количество утечек информации во всех отраслях растет (рис. 1).

**Пителинский Кирилл Владимирович**, доцент кафедры "Информационная безопасность".
E-mail: yekadath@gmail.com
**Федоров Николай Владимирович**, заведующий кафедрой "Информационная безопасность".
E-mail: fedorovnv31@mail.ru
**Чайчиц Анастасия Игоревна**, студентка кафедры "Информационная безопасность".
E-mail: nasta621998@mail.ru
**Широкова Ольга Александровна**, студентка кафедры "Информационная безопасность".
E-mail: Olga143905@yandex.ru

*Статья поступила в редакцию 26 декабря 2019 г.*

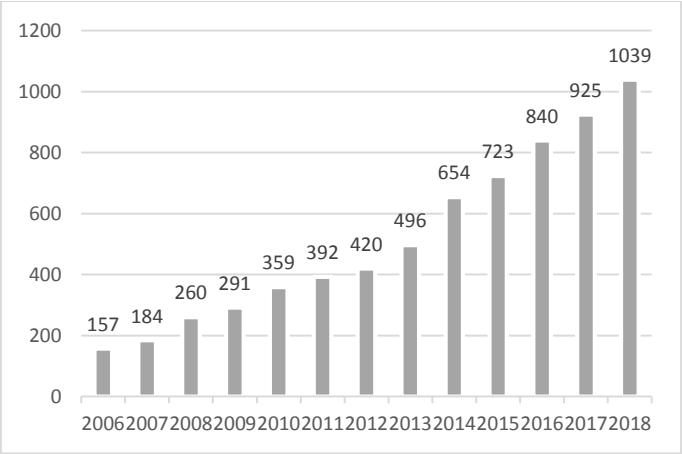



***Рис. 1. Общее число зарегистрированных утечек информации за 2006—2018 гг. [1]***

## Высшее учебное заведение как система контурных потоков

Для повышения результативности и эффективности управления в рамках системного подхода требуется использовать научные методы. Если применительно к сложным социально-экономическим системам вопросы управления еще недостаточно проработаны, то для технических и производственно-технических систем они известны, формализованы и широко применяются.

В контурные потоки вуза [2] входят кадровые, энергетические, финансовые, информационные и материальные потоки, преобразуемые друг в друга при функционировании вуза [3]. Для того чтобы уменьшить риск появления инцидентов и улучшить работоспособность всех структур вуза, можно воспользоваться методом имитационного моделирования и принципом "золотого сечения". Моделирование деятельности вуза как системы контурных потоков (т. е. динамики сложной крупномасштабной системы) представляет собой более трудную задачу, чем моделирование физических систем.

Это обусловлено следующими причинами:

- в расположении исследователя имеется мало фундаментальных физических и математических законов, относящихся к рассмотренной системе;
- многие взаимосвязи между элементами в системе с трудом поддаются количественному описанию и формализации;
- трудно количественно описать поведение входных элементов;
- важную роль играют стохастические процессы;
- неотъемлемой частью таких систем является процесс принятия решений человеком.

На рис. 2 приведена схема возможного подхода к построению модели вуза [4], который трактуется здесь как множество взаимосвязанных элементов, объединенных для выполнения определенной функции. Определение вуза как системы субъективно, поскольку зависит не только от цели разработки модели, но и от системного аналитика (ЛПР).

Процесс моделирования начинается с определения цели разработки модели, по которой затем устанавливаются границы системы и должный уровень детализации моделируемых процессов. Уровень детализации должен позволять абстрагироваться от неточно определенных (из-за недостатка информации) аспектов функционирования реальной системы.

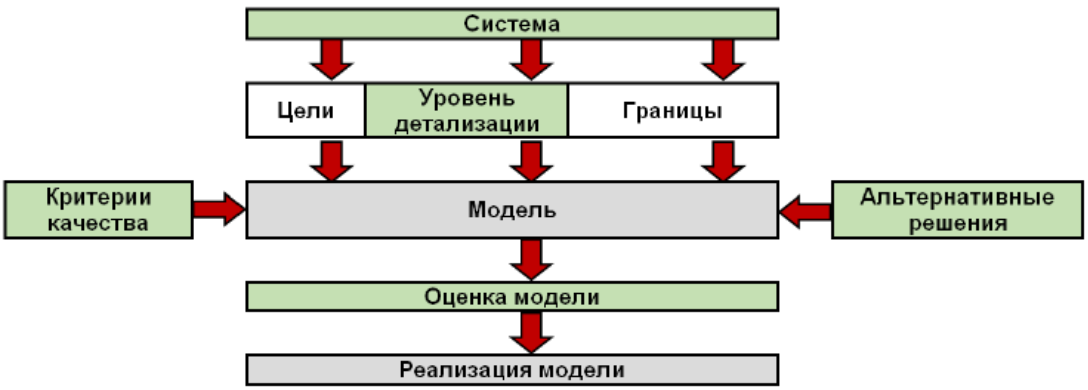



***Рис. 2. Процесс построения модели***

В описание системы должны быть включены критерии эффективности ее функционирования, оцениваемые альтернативные решения (которые могут трактоваться как части модели или как ее входы). Оценки альтернативных решений по заданным критериям эффективности рассматриваются как выходы модели. На практике процесс построения модели является итерационным. После того как на основе полученных оценок альтернатив выработаны рекомендации, можно приступать к внедрению результатов моделирования. При этом в рекомендациях должны быть четко сформулированы как основные решения, так и условия их реализации.

Описанный подход полностью применим к построению имитационных моделей, агрегированных или детализированных. Имитационному моделированию свойственна концепция интерактивного построения модели, при котором модель изменяется путем добавления новых или исключения некоторых ее элементов и (или) взаимосвязей между ними.

Чаще всего вуз не обладает значительными материальными ресурсами. Применяя методы эффективного управления и контроля, можно оптимизировать образовательный процесс, обеспечив тем самым экономическую безопасность реализуемых в вузе бизнес и информационных процессов за счет их непрерывности, например за счет использования "принципа золотого сечения" (см. рис. 2) [5]. Здесь под принципом "золотого сечения" понимается долевое распределение ресурсов внутри уровня иерархии в целом, финансовых ресурсов в пропорции с числами из ряда Фибоначчи (рис. 3).

Однако шаблонно используя метод декомпозиции вуза как системы на составные части, можно столкнуться с тем, что отдельные части этой большой системы перестанут быть адекватно описываемыми по отдельности. Это связано с тем, что отдельные части вуза как организационной системы в рамках синергетического подхода тесно взаимосвязаны друг с другом и не допускают применения к ним методов суперпозиции без утраты для ЛПР части сведений о реализуемых бизнес-процессах, что и обуславливает применение холистического подхода. Поэтому необходимо использовать другой метод управления вузом — системный подход.

Внедрение различных средств и методов биометрической идентификации в контрольную зону вуза позволит его администрации отслеживать параметры циркулирующих в нем контурных потоков (быстро получать сведения обо всех инцидентах за определенный период времени и тем самым купировать возможные негативные последствия) [6].

В такие сведения входят:

- статистика посещения вуза (дата, время);
- доступ работников вуза в контролируемые помещения;
- фиксирование инцидентов внутри контролируемой зоны (всего вуза);
- идентификация работников при работе с определенным оборудованием.

Поскольку территория вуза велика, учебные корпуса, жилые помещения расположены на разных площадках далеко друг от друга, адекватно осуществлять контроль за всей территорией затруднительно. Система биометрической идентификации в таком случае может помочь повысить экономическую и информационную безопасность вуза (о которой далее пойдет речь).

## Информация как нематериальный актив, подлежащий защите

В стоимости предприятий неуклонно растет доля нематериальных активов, эффективное управление которыми становится все более значимым из-за усиления в экономике роли инноваций, интеллектуальных ресурсов, ИТ-технологий и иных аспектов, формулирующих конкурентоспособные бизнес-процессы.

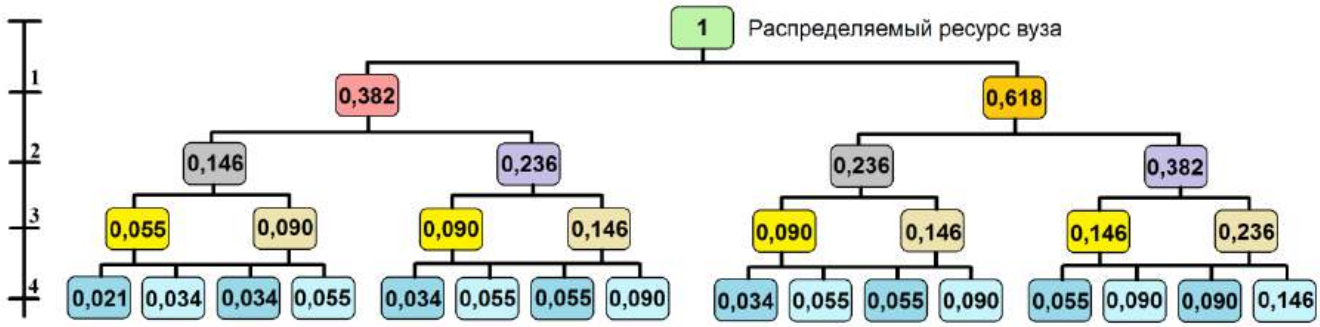



***Рис. 3. "Золотое" распределение ресурсов вуза по четырем иерархическим уровням управления:***
1 — ректорат; 2 — деканаты; 3 — кафедры; 4 — сотрудники

Информация, являясь продуктом деятельности субъектов социально-экономических отношений, считается в таком случае собственностью государства, организация, предприятия, учреждения, граждан и, как любой объект собственности, требует должной защищенности (рис. 4).

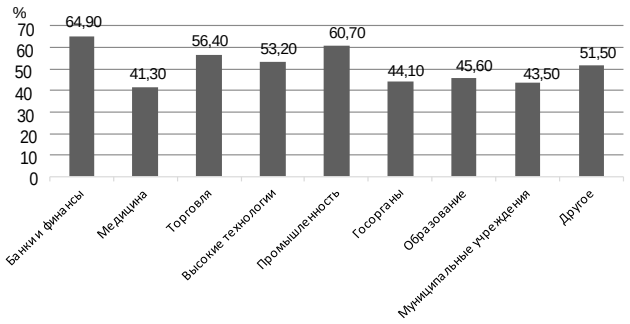



***Рис. 4. Доля умышленных утечек персональных данных (ПДн) от общего числа утечек ПДн по отраслям [1]***

В данном случае под информацией понимается хранение и использование персональных данных пользователей, в частности биометрический код (уникальные личные данные) человека. Незащищенность этих данных грозит их утечкой к третьим лицам и их дальнейшим несанкционированным распространением и использованием для проникновения на защищаемый объект.

В соответствии с ГОСТ Р ИСО/МЭК 17799:2005 Информационная технология. Практические правила управления информационной безопасностью, информация — актив, который подобно другим активам организации имеет ценность и, следовательно, должен быть защищен надлежащим образом (рис. 5).

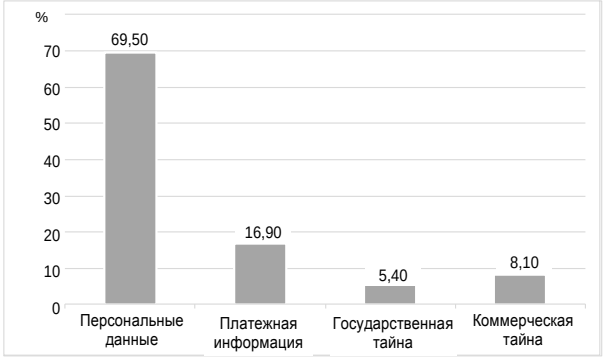



***Рис. 5. Распределение утечек по типам информации 2018 г. [1]***

Перечень персональных данных (ПДн), доступных в личном кабинете студента: ФИО, пол, дата рождения, номер телефона, e-mail, специальность, срок обучения, форма обучения, вид оплаты обучения, адрес проживания.

## Роль персонала в угрозах информационной безопасности и обеспечение непрерывности бизнес-процесса

В основе системы информационной безопасности (ИБ) лежит человеческий фактор, предполагающий склонность персонала к интересам организации и осознанное соблюдение им установленных мер защиты информации. Персонал, владеющий ценной и конфиденциальной информацией, работающий с конфиденциальными данными и документами, является наиболее осведомленным, трудно контролируемым и часто достаточно привлекательным источником для злоумышленника, желающего получить необходимые ему сведения об организации.

Деятельность сотрудников, которая может принести ущерб информационным ресурсам организации, относится к внутренним угрозам безопасности и может быть вызвана различными причинами (некомпетентность или халатность персонала, злой умысел и т. п.). Из-за слабой подготовки кадров, а иногда ввиду отсутствия доскональных и периодических проверок персонала представители предприятий и корпораций становятся целью злоумышленников, которые активно используют приемы социальной инженерии.

Социальная инженерия — совокупность методов и приемов воздействия на человека (должностное лицо, лицо, принимающее решение) для получения конфиденциальной информации путем полного или частичного обхода систем безопасности. Некоторые базовые методы социальной инженерии и меры по противодействию им даны в [7].

Статистически около 50 % случаев злоумышленных действий (покушение на информацию и информационные ресурсы) совершаются людьми, имеющими непосредственный доступ к этой информации (рис. 6). Такие действия совершаются либо по личным мотивам пользователя, либо под воздействием внешнего злоумышленника.

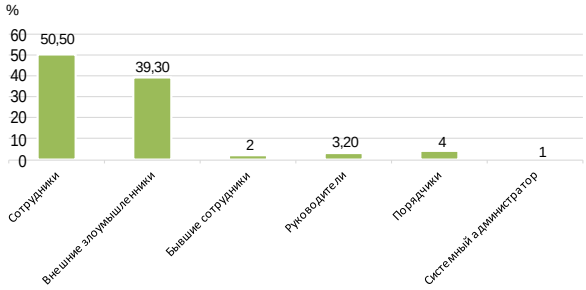



***Рис. 6. Классификация виновников утечек [1]***

На основании отмеченных фактов можно сделать вывод о необходимости защиты информационного контура предприятия (организации) с по-

мощью активного и пассивного воздействия на персонал (как носитель нематериальных активов предприятия) посредством создания и эксплуатации интегрированной автоматизированной системы комплексной безопасности предприятия или организации [8] (рис. 7).

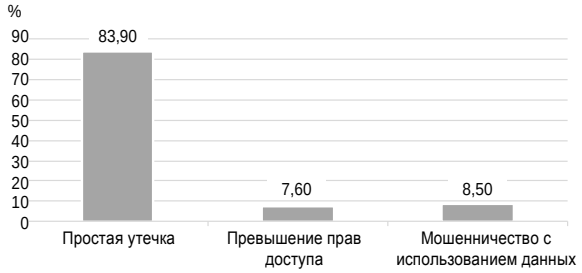



***Рис. 7. Распределение утечек по их характеру [1]***

Один из вариантов решения отмеченных проблем — повышение квалификации сотрудников. Однако руководство зачастую если и отправляет сотрудников на курсы и тренинги для повышения их квалификации и осведомленности, то делает это в ущерб зарплате самих сотрудников. Сотруднику становится выгоднее скорее закончить обучение, чтобы вернуться на рабочее место. Все работники компании должны знать об опасности раскрытия информации и способах ее предотвращения. Сотрудники должны иметь четкие инструкции о том, как и на какие темы говорить с собеседником и какую информацию для точной аутентификации собеседника им необходимо у него получить.

Следовательно, для повышения качества подготовки кадров требуется активная непрерывная консультативно-управленческая деятельность [9], включающая:

- профессиональную подготовку исполнителей;
- координацию действий заинтересованных участников;
- научно-методическую помощь руководителям и специалистам, занятым внедрением инноваций;
- диагностику результатов внедрения социальных технологий;
- корректировку целей и задач процесса внедрения инноваций.

Традиционно эффективная и комплексная ИБ держится на трех видах обеспечения: инженерно-техническом, программно-математическом и организационно-правовом [10].

## Методы и средства биометрической идентификации пользователей

Биометрические методы и средства идентификации пользователей объекта информатизации можно классифицировать как по принципу действия (статические или динамические), так и по биологическому принципу, используемому в процессе идентификации (см. табл. 1).

Таблица 1

**Классификация методов биометрической идентификации**

| Методы идентификации | Биологический признак |
|---|---|
| Статические | Папиллярный узор пальца<br>Радужная оболочка глаза<br>Сетчатка глаза<br>Геометрия лица<br>Геометрия кисти руки<br>Код ДНК |
| Динамические | Голос и особенности речи<br>Динамика почерка и подпись<br>Клавиатурный почерк |
| Комбинированные | Биологические признаки<br>Биологический код совместно с кодом доступа |

Статические методы и средства подразумевают использование биоматериала, не изменяющегося в течение жизни человека (рисунок радужной оболочки глаза, отпечатки пальцев, код ДНК и т. п.). Динамические методы и средства, наоборот, используют признаки, которые могут меняться в течение жизни, но они все равно индивидуальны для каждого человека (голос, почерк и т. п.). Динамические методы использовать сложнее, так как возможность их реализации зависит от многих непрогнозируемых факторов (например, если человек заболел, его голос может меняться; почерк меняется с течением жизни, а клавиатурный почерк необходимо еще выработать на практике).

## Статические методы и средства биометрической идентификации

Статические методы биометрической идентификации основаны на определении человека с помощью его неизменных биометрических характеристик. К статическим методам относят такие характеристики, как папиллярный узор пальца, радужная оболочка и сетчатка глаза, геометрия лица, кисти руки и т. п.

### *Количественные характеристики качества биометрической идентификации*

Качество и достоверность статических методов биометрической идентификации определяют показатели эффективности биометрических систем, так как всегда существует вероятность ошибки (см. табл. 2).

Таблица 2

**Сравнение статических методов и средств биометрической идентификации**

| Метод | Вероятность ошибки | Преимущества | Недостатки |
|---|---|---|---|
| Отпечаток пальца | FAR = 0,001 %, FRR = 0,6 % | Легкость в использовании<br>Высокий уровень надежности и достоверности<br>Низкая стоимость оборудования<br>Высокая скорость идентификации<br>Высокая доступность на рынке | Нарушение папиллярного узора мелкими царапинами и порезами<br>Невозможность считывания данных при загрязнении оборудования<br>Высокая вероятность фальсификации данных |
| Радужная оболочка глаза | FAR = 0,00001 %, FRR = 0,016 % | Высокая скорость идентификации<br>Невозможность подделки биометрических данных | Высокая стоимость оборудования<br>Низкая доступность на рынке РФ |
| Сетчатка глаза | FAR = 0,0001 %, FRR = 0,4 % | Низкий уровень ошибок,<br>Высокая точность сканирования<br>Невозможность подделки биометрических данных | Высокая стоимость оборудования<br>Низкий комфорт пользователя<br>Низкая скорость идентификации |
| Геометрия лица (2 D) | FAR = 0,1 %, FRR = 2,5 % | Отсутствие прямого контакта с устройством<br>Высокая скорость идентификации<br>Распознавание на большом расстоянии<br>Высокий комфорт пользователя | Сложность распознавания при слабом освещении<br>Распознавание только под некоторыми углами и ракурсами<br>Чувствительность к изменениям лица (мимика, аксессуары) |
| Геометрия лица (3 D) | FAR = 0,0005 %, FRR = 0,1 % | | |
| Геометрия кисти руки | FAR = 0,0008 %, FRR = 0,01 % | Высокая скорость идентификации<br>Высокая доступность на рынке | Большие размеры сканирующего устройства<br>Сканирование на маленьком расстоянии |

Показатели эффективности биометрических систем:

- FAR (False Acceptance Rate — вероятность ложного допуска) — вероятность того, что произойдет ошибка и система распознает человека, не зарегистрированного в базе данных (БД);
- FRR (False Rejection Rate — вероятность ложного недопуска) — в противоположность FAR обозначает вероятность того, что система может ошибочно отказать в доступе человеку, зарегистрированному в БД.

### *Идентификация по папиллярным линиям пальца*

Метод является одним из самых распространенных и основан на сравнении конкретных точек узора папиллярных линий (поскольку у каждого человека свой уникальный узор). Залогом дальнейшего развития метода является его частое использование в криминалистике. Алгоритм работы метода основан на сканировании устройством отпечатка пальцев, преобразовании его в цифровой код и сравнении его с шаблоном, зарегистрированным в дактилоскопической БД. Время считывания кода обычно составляет около секунды и зависит от размера шаблона в таблице (время поднесения пальца к сканеру не учитывается).

Выделяют три типа папиллярных узоров (см. рис. 8, 9):

- с 1 по 4: узоры типа "петля" (левая, правая, центральная, двойная);
- 5 и 6: узоры типа "дельта" или "дуга" (простая и острая);
- 7 и 8: узоры типа "спираль" (центральная и смешанная).


***Рис. 8. Типы папиллярных узоров [12]***

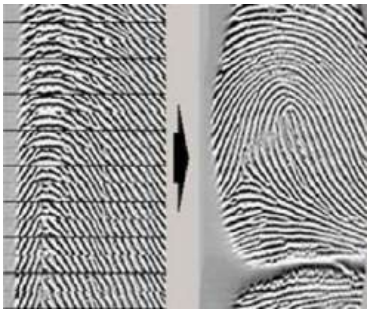


***Рис. 9. Покадровое считывание картины отпечатка пальца и его реконструкция [13]***

*Идентификация по радужной оболочке глаза и сетчатке глаза*

Эти методы имеют наиболее точные показатели среди всех остальных биометрических методов. Радужная оболочка глаза является уникальной особенностью человека. Алгоритм метода основан на том, что камера настраивается на глаз и с помощью монохромного сканера, который использует инфракрасный свет низкой интенсивности, разбивает изображение на множество блоков и поочередно сравнивает их с шаблонами в БД (рис. 10).

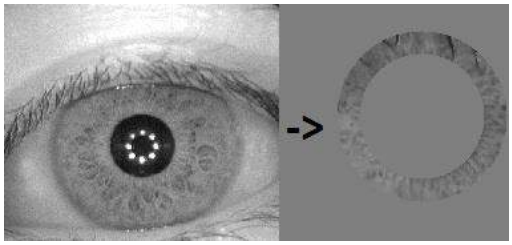


***Рис. 10. Выделение радужной оболочки глаза [14]***

*Идентификация по геометрии лица*

Данный метод является одним из самых привычных для человека, так как основой для него служит использование удостоверения личности с фотографией (паспорт). Метод можно классифицировать на 2D и 3D-распознавание личности (рис. 11).

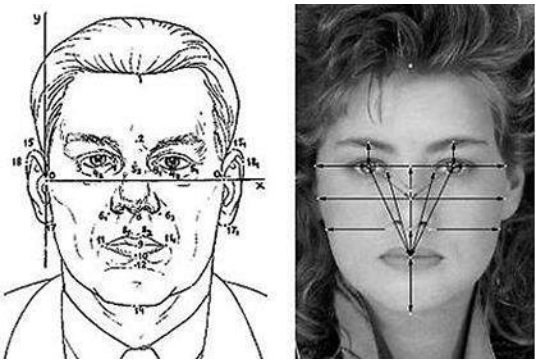


***Рис. 11. Выделение ключевых точек в 2 D методе сканирования геометрии лица [15]***

Метод 2D признан одним из неэффективных методов биометрии: он не учитывает некоторые изменения во внешности с течением времени (изменение прически, мимики, усы и т. д.). Несмотря на данные недостатки, он продолжает использоваться из-за сравнительно низкой стоимости оборудования. Алгоритм работы метода основан на сравнении некоторых точек на лице, расстояния между ними и последующего сравнения с шаблонами из БД.

В основе 3D-распознавания лежит построение объемного шаблона лица человека за счет того, что на лицо проецируется некая сетка и делается множество снимков, снятых с разных углов для создания образа лица, который в дальнейшем также сравнивается с теми, что представлены в БД.

*Идентификация по геометрии кисти руки*

Метод по своей технологической структуре и уровню надежности подобен методу идентификации личности по отпечатку пальца. Статистическая вероятность существования двух кистей рук с одинаковой геометрией чрезвычайно мала. Однако признаки руки меняются с возрастом, а само устройство довольно велико (рис. 12).

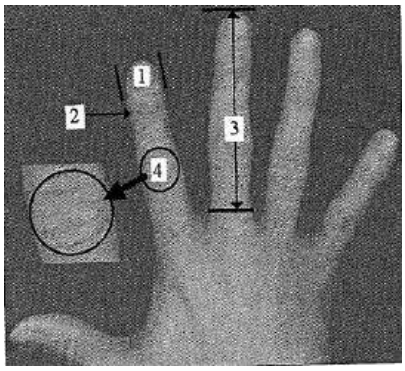



***Рис. 12. Ключевые характеристики для идентификации по геометрии руки [15]***

Компания Fujitsu использовала в своих разработках технологию сканирования вен (обычно применяется в медицинских учреждениях). Технология была названа PalmSecure. В ее основе лежит метод сканирования вен ладони руки. Получаемый рисунок имеет большее количество уникальных областей для идентификации, а его надежность сопоставима с технологией идентификации по радужной оболочке глаза (рис. 13).

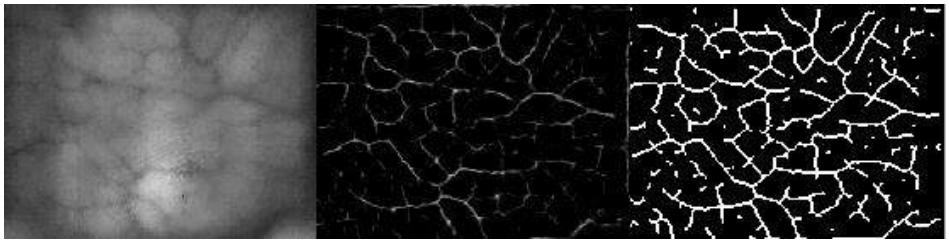


***Рис. 13. Выделение рисунка вен ладони руки [16]***

## Динамические методы и средства биометрической идентификации

Динамические методы биометрической идентификации основаны на определении человека по его поведению во время определенного действия. К динамическим методам относят следующие виды биометрии: особенности голоса, динамика почерка, клавиатурный почерк и т. д.

*Идентификация по голосу и особенностям речи*

Идентификация по голосу реализуется с помощью выявления определенных характеристик голоса человека и сравнения их с образами из БД. Учитываются такие характеристики, как особенности речи, произношение, тональность, громкость.

Для того чтобы описать голос как сложную звуковую волну, необходимо использовать преобразование Фурье (рис. 14).

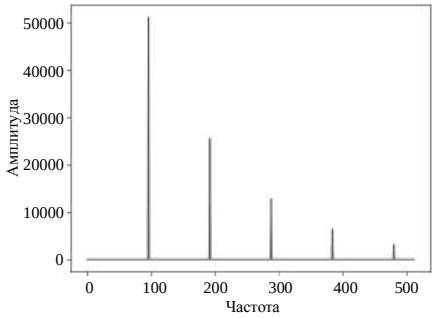



***Рис. 14. Преобразование Фурье от синуса [17]***

Кроме основного пика, который представляет собой сигнал, на графике есть меньшие пики (гармоники), которые, по сути, не несут какой-либо полезной информации. Соответственно первую спектрограмму необходимо логарифмировать, чтобы получить спектрограмму второго порядка. В итоге на логарифмированной спектрограмме видны пики одинакового размера (рис. 15).

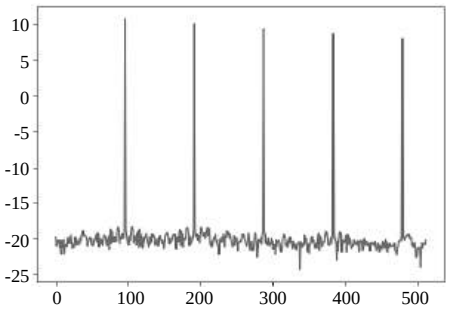


***Рис. 15. Логарифм спектрограммы [17]***

Математический способ позволяет описать звуковую волну как спектрограмму в частотно-амплитудном виде. Однако помимо основных частот при этом возникают гармоники, которые мешают анализу (дублируют информацию). Для устранения этого рассчитывается спектрограмма от спектрограммы (кепстр). По формуле $m = 1127\ln(1 + f / 700)$ можно высчитать величину мел (психофизическая единица высоты звука, применяемая в музыкальной акустике), которая отражает способность распознавать разные частоты (рис. 16). В данной формуле используется обратное преобразование. По определению частота звука 20 Гц, а уровень громкости 40 фон (единица измерения уровня громкости звука).

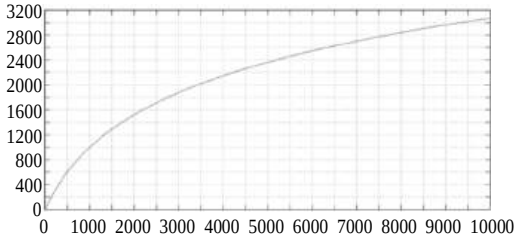


***Рис. 16. Зависимость высоты звука в мелах от частоты колебаний [17]***

Алгоритмически реализовав эту методику, можно обрабатывать записанные звуковые волны, что и будет являться уникальным "отпечатком" голоса. При идентификации по голосу компьютер обрабатывает входные звуковые волны в режиме реального времени и сопоставляет их с содержимым БД.

*Идентификация по динамике почерка и подписи*

Пока подпись человека — уникальный и стабильный атрибут его идентификации (рис. 17, 18). В частности, ее можно перевести в цифровой вид и подвергнуть компьютерной обработке. Однако цифровую подпись (из-за ее специфических характеристик) нельзя использовать для ограничения доступа в помещения или для доступа в компьютерные сети.

***Рис. 17. Планшет для точного захвата рукописной подписи от SignotecGmbH***

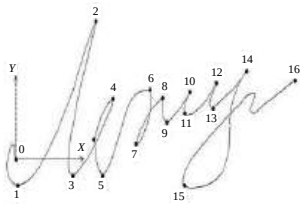


***Рис. 18. Подпись, введенная с помощью графического планшета [18]***

Идентификация по почерку использует следующие характеристики при написании и идентификации человека: размер, наклон, нажим (рис. 19—21).

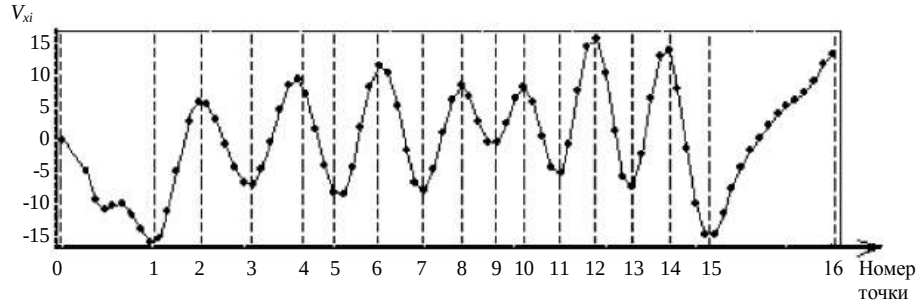



***Рис. 19. Динамика колебания пера по оси X введенной подписи на планшете [18]***

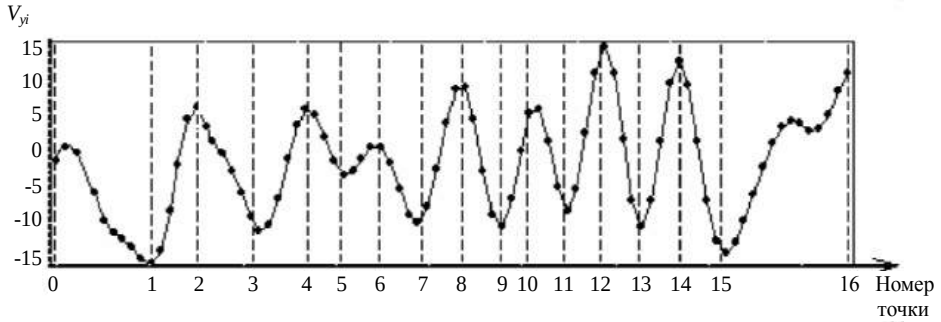



***Рис. 20. Динамика колебания пера по оси Y введенной подписи на планшете [18]***

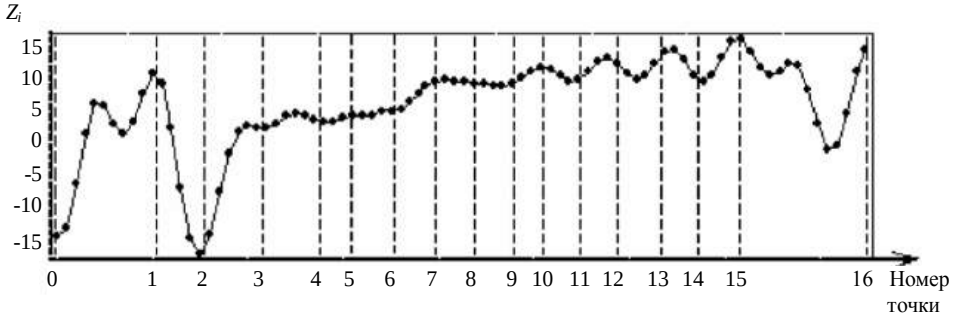



***Рис. 21. Динамика колебания пера по оси Z введенной подписи на планшете (сила нажима на кончик пера) [18]***

Более сложный метод идентификации по динамике почерка осуществляется путем написания от руки минимум трех строчек текста. Однако этот метод допускает риск того, что найдется минимум один человек, который сможет повторить структуру почерка, и соответственно не является полностью безопасным для идентификации человека.

*Идентификация по клавиатурному почерку*

Для того чтобы реализовать данный тип идентификации, необходимо ввести либо ключевую фразу, либо произвольный текст и зафиксировать нужные характеристики для идентификации человека.

К характеристикам идентификации по клавиатурному почерку относят:

- временные интервалы;
- время удержания определенных кнопок;
- частоту возникновения ошибок;
- нажатие (плавное или резкое).

Вначале необходимо зафиксировать ключевые значения в БД для дальнейшего сопоставления. Делается это путем многочисленного ввода определенных фраз или текста человеком. Алгоритм работы заключается в ведении диаграммы частот использования биграмм (статистике) с указанием времени удержания первой клавиши биграммы, второй и паузы между этими двумя нажатиями (табл. 3).

После "обучения" системы можно создать диаграмму анализа данных, которая заносится в БД для дальнейшего использования. Для идентификации человек вводит ключевую фразу или текст, по которому система может сопоставить временные рамки с находящимися в БД (табл. 4).

Таблица 3

**Пример скорости печати текста одним пользователем (на примере биграмм)**

| Биграммы | Время удержания первой клавиши | Время удержания второй клавиши | Пауза между нажатиями |
|---|---|---|---|
| ан/на | 64 | 70 | 120 |
| ос/со | 65 | 82 | 121 |
| ен/не | 65 | 71 | 185 |
| од/до | 64 | 64 | 127 |
| ка/ак | 63 | 74 | 145 |
| но/он | 65 | 74 | 201 |
| ов/во | 68 | 65 | 150 |
| ил/ли | 65 | 66 | 197 |
| ни/ин | 63 | 81 | 140 |
| ет/те | 64 | 63 | 120 |
| то/от | 62 | 73 | 96 |
| пр/рп | 61 | 65 | 87 |
| та/ат | 65 | 81 | 104 |
| ис/си | 61 | 61 | 200 |
| но/он | 61 | 72 | 99 |

Таблица 4

**Оценка стабильности клавиатурного почерка пользователя**

| Ошибка | Аритмичность | Число знаков в минуту | Число перекрытий | Используемое число пальцев | Оценка |
|---|---|---|---|---|---|
| <2 % | < 10 % | > 200 | > 50 % | 10 | 5/5 |
| <4 % | < 15 % | > 150 | > 30 % | > 5 | 4/5 |
| <8 % | < 20 % | > 100 | > 10 % | < 5 | 3/5 |
| >8 % | > 20 % | < 100 | < 10 % | По 1 | 2/5 |

## Заключение

Из-за наметившегося повсеместного перехода к цифровой экономике (в т. ч. и в сфере образования) необходимо изменить общий подход к управлению вузом вообще и к организации образовательного и иных бизнес-процессов. Главным направлением развития образовательных процессов становится человеческий фактор, отчего, в частности, требуется пересмотреть сложившийся подход к функционированию образовательных систем и комплексов.

Наработанный инструментарий математического и имитационного моделирования позволяет получать не только количественные, но и качественные характеристики динамики бизнес-процессов в интересующем их владельцев разрезе. Одним из способов описания деятельности организации является модель в виде взаимодействия динамических контурных потоков (информационных, финансовых, материальных, энергетических и кадровых). Для их защиты необходимо использовать весь комплекс мер и средств по обеспечению экономической и информационной безопасности.

Для того чтобы обеспечить надежность защиты информации в информационном контуре вуза, требуются новейшие технологии защиты информации, такие как методы идентификации и аутентификации. В частности, с помощью биометрических средств идентификации можно добиться высокого уровня защищенности информационных ресурсов вуза от несанкционированного доступа, копирования, модификации и блокировки (уничтожения) информации. Так удастся сохранить непрерывность реализуемых вузом бизнес-процессов, что, в свою очередь, обеспечит ему должную конкурентоспособность на рынке образовательных услуг.

**Литература**


1. Infowatch: [Электронный ресурс]. URL: https://www.infowatch.ru (дата обращения: 06.12.2019).
2. *Пителинский К. В.* О системе динамических контурных потоков организации: Устойчивое инновационное развитие: проектирование и управление. Т. 3 2009 [Электронный ресурс]. URL: http://www.rypravlenie.ru/?cat=11 (дата обращения: 06.12.2019).
3. *Пителинский К. В.* Управление рисками деятельности компании с помощью оптимизации ее динамических контурных потоков // Оборонный комплекс — научно-техническому прогрессу России. 2016. Вып. 4. С. 53—60.
4. *Федоров Н. В.* Математическое и имитационное моделирование сложных систем: учеб. пособие. — МГИУ, 2015. С. 212.
5. *Пителинский К. В.* Моделирование динамических контурных потоков как метод управления непрерывностью бизнеса // Методы менеджмента качества. 2018. № 11. С. 16—21.

6. *Пителинский К. В., Плоткин А. С., Кривоногов А. А.* О некоторых методах и средствах развития и защиты ресурсов вуза, обеспечивающих непрерывность его деятельности // Вопросы защиты информации. 2019. № 2. С. 53—59.

7. *Ермаков И. К., Ермолатий Д. А., Пителинский К. В.* Социальная инженерия как технология нарушения информационной и экономической безопасности субъекта экономики // Вестник московской международной академии. 2019. № 1. С. 74—83.

8. *Пителинский К. В., Антипенкова А. А., Титов В. Р.* Защита информации на предприятии как средство минимизации рисков его инвестора // Межотраслевая информационная служба. 2014. Вып. 1. С. 68—78.

9. *Зинченко Г. П.* Государственная служба и социальная инженерия [Электронный ресурс]. URL: https://cyberleninka.ru/article/v/gosudarstvennaya-sluzhba-v-pole-sotsialnoyinzhenerii (дата обращения: 01.05.2018).

10. *Родичев Ю.* Нормативная база и стандарты в области информационной безопасности. — СПб: Питер, 2017. С. 254.

11. *Карцан Р. В., Карцан И. Н.* Дактилоскопия. Биометрический метод идентификации на режимном предприятии // Актуальные проблемы авиации и космонавтики. 2013. № 9. С. 405—406.

12. *Брюхомицкий Ю. А.* Биометрические технологии идентификации личности. Контроль доступа по папиллярному узору, 2017. С. 38.

13. *Ламберт Е.* Считыватель отпечатков пальцев FingerChip корпорации Atmel // Электронные компоненты. 2005. № 5. С. 60—65.

14. *Павельева Е. А., Крылов А. С.* Алгоритм идентификации человека по ключевым точкам радужной оболочки глаза: 19-я Межд. конф. по компьютерной графике и ее приложениям ГрафиКон' 2009. — М., 2009. С. 228—231.

15. *Мальцев А.* Современные биометрические методы идентификации [Электронный ресурс]. URL: https://habr.com/ru/post/126144 (дата обращения: 11.08.2011).

16. Биометрическая идентификация по рисунку вен ладони [Электронный ресурс]. URL: https://habr.com/ru/post/149424 (дата обращения: 11.08.2012).

17. *Киреев М.* Машинный слух. Как работает идентификация человека по его голосу [Электронный ресурс]. URL: https://xakep.ru/2019/09/03/voice-recognition (дата обращения: 03.09.2019).

18. *Ложников П. С.* Идентификация человека по динамике написания слов в компьютерных системах // Успехи современного естествознания. 2004. Вып. 4. С. 129—130.

# Management of the information circuit of the university and its protection using biometric identification: some methods and tools

*K. V. Pitelinsky, N. V. Fedorov, A. I. Chaychits, O. A. Shirokova*
Moscow Polytechnic University, Moscow, Russia

*The necessity of optimizing and protecting the contour flows circulating in a university by using the biometric identification subsystem of staff and students in an automated university management system is discussed (in particular, to reduce the percentage of information leaks). Existing methods and means of biometric identification are considered.*

*Keywords:* information security, university management, biometrics, dynamic contour flows, ACS, simulation, "golden ratio".

Bibliography — 18 references. *Received December 26, 2019*

## ДОВЕРЕННАЯ СРЕДА

УДК 004.056

# Разработка подхода к мониторингу безопасности IoT-устройств на базе MQTT-брокера

[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 разработке способа мониторинга безопасности устройств Интернета вещей (IoT), в основе которого лежит использование концепции функционирования MQTT-брокера применительно к мониторингу безопасности. Для рассмотрения данной темы изучена зарубежная практика в области Интернета вещей. Предложен способ мониторинга с использованием шаблона передачи данных "издатель—подписчик", получением и обработкой данных мониторинга во времени, близком к реальному, и безагентной реализацией подключения устройств. Рассмотрены варианты реализации способа и преимущества использования IoT-ориентированного протокола передачи данных.*

*Ключевые слова*: кибербезопасность, IoT, Интернет вещей, мониторинг безопасности, инциденты.

Согласно исследованию [1] около 97 % опрошенных организаций беспокоит безопасность систем Интернета вещей (*Internet of things* — IoT). Отслеживание состояния IoT-устройств и их управление признано одной из наиболее перспективных превентивных мер, поскольку даже минимальный мониторинг позволит выявить существующие проблемы и нарушения информационной безопасности (ИБ), устранение которых позволит повысить уровень безопасности IoT-сети.

В контексте обеспечения безопасности IoT-устройств необходимость мониторинга безопасности всех устройств и проверки их показателей остается недостаточно рассмотренной. Различные компании предлагают свои продукты по аналитике, основная часть которых позволяет акцентироваться на анализе информации из журналов на уровне облачных хранилищ и IoT-инфраструктуры. При этом их базовый аналитический инструментарий часто расширяют с помощью технологий искусственного интеллекта, машинного обучения и интеграции с платформами Больших данных [2].

**Иванов Павел Алексеевич**, бакалавр.
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 28 января 2020 г.*



Большинство IoT-устройств подключают друг к другу напрямую, в обход центрального сервера. При этом облачную платформу используют для управления и сбора статистики. Это размывает периметр информационной безопасности и заставляет пересмотреть подходы к его защите. Кроме того, подавляющее большинство устройств IoT независимо от их типа подключения к сети не контролируются и ограничены в ресурсах. Они не имеют возможности запускать на своей стороне традиционные решения для мониторинга, такие как агентское программное обеспечение, или же они не могут сканироваться удаленно. Поэтому традиционные продукты для обеспечения безопасности конечных точек и устаревшие средства контроля доступа к сети не работают в большинстве случаев использования IoT-устройств [3].

В результате возникает необходимость разработки концепции мониторинга безопасности, который будут осуществлять на уровне IoT-сети, а не на уровне платформы или облака. Основой такой концепции должен стать безагентный способ сбора и аналитики информации, поступающей от IoT-устройств. Это позволит обнаруживать подозрительную активность устройств, для чего имеющиеся средства не обладают достаточной эффективностью.

Цель данной работы — рассмотрение способа мониторинга безопасности IoT-устройств, который позволит получать информацию непосредственно от самих устройств по протоколу MQTT (*Message Queuing Telemetry Transport*) [4], прово-

дить синтаксический анализ поступающей информации и выделять из нее те события, которые относятся к инцидентам и событиям безопасности.

IoT-устройства из-за темпов развития и своей специфики требуют анализа существующей модели угроз информационной безопасности, а также выделения признаков ряда нестандартных угроз, характерных только для IoT-устройств. По данным Лаборатории Касперского [5], за первую половину 2018 г. получено в три раза больше образцов вредоносного программного обеспечения (ПО), атакующего "умные" устройства, чем за весь 2017 г. Диаграмма количества образцов вредоносного ПО приведена на рис. 1.

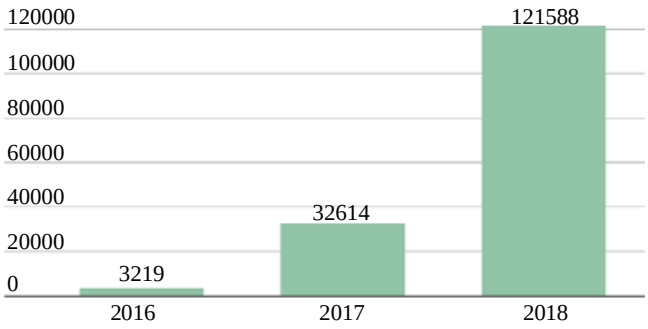



***Рис. 1. Количество образцов вредоносного ПО для IoT-устройств за 2016—2018 гг.***

Исследование данного вопроса может заключаться в анализе взаимодействия IoT-устройств и существующих способов их мониторинга, выделении ряда признаков проявления угроз, характерных для IoT-инфраструктуры, и разработке способа мониторинга безопасности, основанного на концепции MQTT-брокеров и функционирующего по принципу очередей сообщений.

Векторы атак, используемые злоумышленниками для заражения "умных" устройств, характерны и для более традиционных рабочих станций, серверных машин и сетевого оборудования. Для них уже известны характерные события, говорящие о том, что происходит попытка реализации угрозы. Однако в контексте использования IoT-устройств вопросы мониторинга безопасности не получили должного рассмотрения и изучения. Опора только на известные практики по выявлению инцидентов может оказаться неэффективной, поэтому для IoT-устройств требуется проведение анализа ландшафта современных угроз и конкретизация соответствующих признаков для использования в разрабатываемой концепции мониторинга.

Кроме того, мониторинг безопасности должен быть применим к сложным гетерогенным сетям IoT, использующим разные транспортные протоколы передачи данных, что обеспечит видимость всех активных устройств и вырабатываемых ими событий. Это ставит задачу выбора оптимальной архитектурной модели с использованием такого шаблона взаимодействия, который обеспечит подключение IoT-устройств к модулю мониторинга в различных информационных системах. Платформа мониторинга должна быть выбрана и внедрена таким образом, чтобы обеспечить достаточный контроль устройств и обработку данных в сетях IoT.

Реализация предлагаемого способа мониторинга подразумевает внедрение в локальную инфраструктуру IoT брокера мониторинга безопасности, который послужит узлом, получающим сообщения от IoT-устройств в рамках подписки, обеспечиваемой протоколом MQTT, получившим широкое распространение, который де-факто является основой построения IoT-систем [6].

Выбор данного протокола также удовлетворяет требованиям безопасности, так как он работает поверх стандартного протокола TCP (*Transmission Control* Protocol) и предполагает использование механизмов аутентификации и шифрования транспортного протокола TLS/SSL [7].

Способ мониторинга IoT-устройств характеризуется сбором данных "брокером мониторинга безопасности" в рамках передачи "издатель—подписчик", а также получением и обработкой данных мониторинга во времени, близком к реальному, и возможностью реализации мониторинга устройств, которые не могут быть подключены к системе мониторинга посредством агентов.

На брокера могут быть возложены как полный функционал по обработке и анализу событий, так и функции шлюза, осуществляющего первичную обработку сообщений и передачу на выделенный сервер. На рис. 2 представлен один из способов интеграции брокера в типичную инфраструктуру информационной системы (ИС).

Данный способ имеет ряд преимуществ перед традиционными средствами мониторинга, которые вытекают из спецификации способа мониторинга под взаимодействие устройств IoT и их инфраструктуру. Среди преимуществ можно выделить следующие:

- возможность подключения всех используемых устройств за счет безагентной передачи сообщений;
- малый объем передаваемых сообщений;
- гибкая интеграция и масштабирование за счет простого подключения источников событий;
- гарантия доставки всех сообщений брокеру благодаря QoS (от англ. *Quality of Service*);
- обработка большого количества событий без потери при внедрении балансировщиков нагрузки.

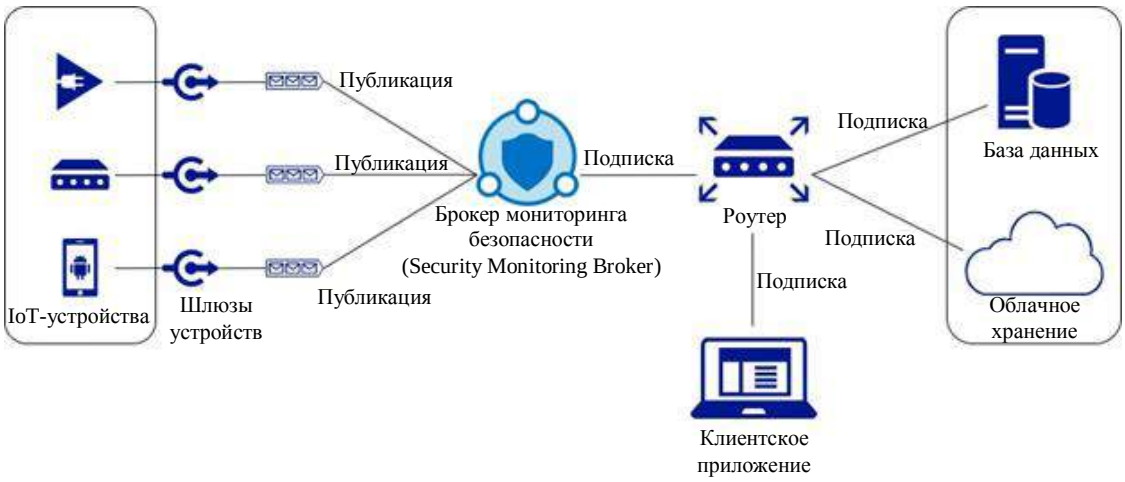



***Рис. 2. Схема интеграции брокера мониторинга безопасности в ИС с простой архитектурой***

Рост количества "умных" устройств и развитие всей отрасти IoT приводят к тому, что в угоду функциональности их безопасности уделяют недостаточно внимания. Все это делает IoT-устройства благоприятной целью для злоумышленников. Своевременное обнаружение инцидентов безопасности позволит избежать негативных последствий и даст понимание картины состояния защищенности IoT-устройств. Предложенный способ мониторинга безопасности позволит решить данную проблему и обеспечить более высокий уровень прозрачности и защищенности IoT-инфраструктуры.

**Литература**

1. IoT Signals Report [Электронный ресурс]. URL: https://azure.microsoft.com/ru-ru/resources/iot-signals/ (дата обращения: 18.10.2019).

2. Six Internet of Things (IoT) security technologies on the contemporary market [Электронный ресурс]. URL: https://medium.com/datadriveninvestor/6-internet-of-things-iot-security-technologies-on-the-contemporary-market-8b302d04d1d0 (дата обращения: 08.11.2019).

3. IoT security: the majority of IoT devices is not monitored in real time [Электронный ресурс]. URL: https://www.i-scoop.eu/iot-security-majority-iot-devices-not-monitored-real-time/ (дата обращения: 07.11.2019).

4. Documentation. Protocol Specifications [Электронный ресурс]. URL: http://mqtt.org/documentation (дата обращения: 20.10.2019).

5. Новые тренды в мире IoT-угроз [Электронный ресурс]. URL: https://securelist.ru/new-trends-in-the-world-of-iot-threats//91601/ (дата обращения: 20.10.2019)

6. Платформа ARM и брокер MQTT как современная основа решений для Интернета вещей [Электронный ресурс]. URL: https://m.habr.com/ru/company/unet/blog/407867/ (дата обращения: 19.10.2019).

7. Проектирование и построение защищенных IoT-решений. Ч. 1. Защита IoT-устройств и шлюзов [Электронный ресурс]. URL: https://www.ibm.com/developerworks/ru/library// iot-trs-secure-iot-solutions1/index.html (дата обращения: 19.10.2019).

## Development of a security analysis approach of IoT-devices based on MQTT-broker

[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 a development approach of security analysis of IoT-devices based on MQTT-broker. The analysis of this subject (approach) focuses on examination of foreign practices in IoT sphere. This article offers a method of IoT security analysis based on "publisher-subscriber" pattern, near-real time receiving and processing of data and agentless implementation of connecting devices. Variants of the approach implementation and benefits of using IoT-oriented MQTT protocol are also considered.*

*Keywords:* cybersecurity, IoT, Internet of things, security analysis, incidents.

Bibliography — 7 references. *Received January 28, 2020*

УДК 004.93

# Методы распознавания личности на основе анализа характеристик наружного уха
*(Обзор)*

*И. М. Гарипов*
ФГАОУ ВО «Национальный исследовательский университет ИТМО», Санкт-Петербург, Россия

*А. Е. Сулавко*, канд. техн. наук; *И. А. Куприк*
ФГБОУ ВО «Омский государственный технический университет», г. Омск, Россия

*Описаны подходы к извлечению признаков биометрических параметров уха на двумерном и трехмерном изображениях, а также на основе измерений передаточных функций ушного канала. Изучены используемые методы распознавания образов для построения средств биометрической идентификации и аутентификации по параметрам ушной раковины, приведены основные результаты исследований.*

*Ключевые слова:* аутентификация, биометрия, идентификация личности, определение ушной раковины на изображении, извлечение признаков, распознавание образов.

С начала XXI века все больше внимания уделяется распознаванию личности на основе биометрических параметров человека. Начало исследований в области биометрии было положено в XX в., толчком к стремительному развитию данной отрасли стали трагические события 11 сентября 2001 г. Согласно прогнозам ведущих аналитических агентств мира, к 2022 г. объем рынка биометрических систем составит 40 млрд долл. В России актуальность исследований в области биометрии обусловлена рядом научно-технических задач Национальной технологической инициативы (НТИ).

Переход к цифровой экономике невозможен без должного уровня развития технологий биометрической идентификации и аутентификации. Наиболее широкое распространение получили системы, основанные преимущественно на анализе открытых биометрических образов — отпечатка пальца, геометрии ладони, лица, радужной оболочки глаза, голоса (без учета семантики речи). Особое внимание многих исследователей сосредоточено на разработке методов распознавания личности по особенностям строения ушной раковины [1—3].

Анатомические исследования показывают, что формирование человеческого уха происходит в период от 4 месяцев до 8 лет, а затем уши растут очень медленно и пропорционально. Некоторые параметры уха, такие как мочка и козелок, меняются со временем незначительно, остальные остаются почти неизменными, что позволяет использовать эти параметры в целях биометрической идентификации и аутентификации субъекта.

Важнейшим свойством аутентификатора является его секретность. В этом смысле традиционные статические биометрические характеристики являются уязвимыми. В частности, отпечатки пальцев остаются на предметах, а изображения лиц — на фотографиях. Злоумышленник может скопировать ключевые особенности биометрического образа и синтезировать фальсификат. Таким образом, эти характеристики нельзя держать в тайне, а значит, и использовать в целях аутентификации (только для идентификации). Основная часть индивидуальных особенностей уха человека расположена в ушной раковине и скрыта от непосредственного наблюдения, поэтому не может быть скопирована бесконтактно или скрытно от владельца, а также путем фотографирования ("плоское изображение" уха ненадлежащего качества, как правило, неинформативно для целей изготовления "муляжа").

## Общая информация о методах распознавания личности по параметрам уха

Биометрические системы идентификации/аутентификации по особенностям строения ушной раковины могут различаться в зависимости от используемого считывающего устройства. Обычно считывающим устройством является камера (CCTV), а элементом обработки — 2D-изображение. Помимо фотографирующих средств для считывания могут быть использованы 3D-сканеры [4], а также наушники [5].

**Гарипов Ильнур Мидхатович**, магистрант.
E-mail: i_garipov@mail.ru
**Сулавко Алексей Евгеньевич**, доцент кафедры "Комплексная защита информации".
E-mail: sulavich@mail.ru
**Куприк Ирина Александровна**, магистрант.
E-mail: ann.ik@mail.ru

*Статья поступила в редакцию 19 декабря 2019 г.*

Вне зависимости от типа биометрической системы (2D, 3D) процедура распознавания пользователя включает в себя несколько этапов: ввод характеристик ушной раковины, предварительная обработка биометрического образа, извлечение признаков, сравнение с эталоном. При обучении системы (создании эталона) необходимо ввести один или несколько примеров образа. При этом этапы ввода, предварительной обработки и извлечения признаков, как правило, не имеют принципиальных отличий.

На этапе предварительной обработки образа часто происходит обнаружение так называемой области интереса (Region-of-interest, ROI) — фрагмента образа, который непосредственно содержит основную информацию о субъекте. Эта процедура является одной из наиболее важных в общем конвейере обработки, значительно влияющей на производительность всей системы распознавания [6].

Показатели надежности любой биометрической системы аутентификации или идентификации выражены в вероятностях ошибок 1-го и 2-го рода. Ошибка 1-го рода (False Rejection Rate, FRR) представляет собой ложный отказ в допуске зарегистрированного пользователя, ошибка 2-го рода (False Acceptance Rate, FAR) характеризует ложный допуск любого неизвестного пользователя. Когда обе вероятности равны (FRR = FAR), говорят о равной вероятности ошибок (Equal Error Rate, EER).

### Методы распознавания субъектов по двумерному изображению уха

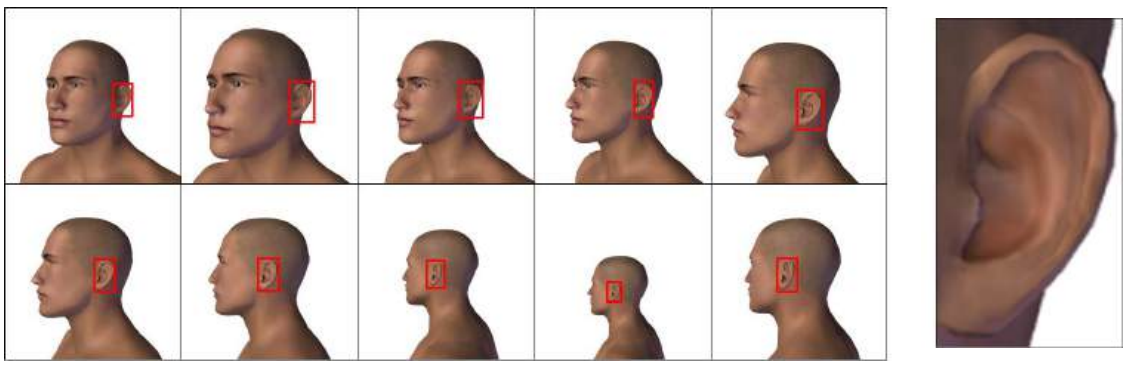
Этот тип систем распознавания в качестве входных данных использует изображения (видеопоток), которые обычно получают с фото- и видеокамер. Процесс предварительной обработки изображений ушной раковины, называемый нахождением (детектированием), обычно включает в себя обнаружение ушной раковины на входном изображении (рис. 1, *а*), сегментацию и нормализацию на (рис. 1, *б*). В общем случае под нормализацией понимают приведение обработанных изображений к единому размеру.

Изображение может содержать не только образы "чистого" уха, но и другие элементы (например, профиль лица, посторонних людей). Также возможна частичная окклюзия (сокрытие) ушей, например посредством украшений, очков или волос. В связи с этим задача обнаружения уха на входном изображении становится затруднительной.

В работе [7] предложен метод автоматического обнаружения уха на основе алгоритма AdaBoost (Adaptive Boosting, адаптивный бустинг — семейство алгоритмов машинного обучения, объединяющих каскад слабых обучающих классификаторов к сильному). В работе "слабые" классификаторы построены на использовании примитивов Хаара, позволяющих обнаружить вертикальные и горизонтальные края уха. Сильный классификатор создается путем объединения набора выбранных слабых классификаторов с использованием алгоритма AdaBoost. Алгоритм использует обучение с учителем с помощью метода обертывания. Он выбирает лучший слабый классификатор с учетом заданной взвешенной ошибки входных выборок на каждой итерации. По результатам эксперимента по распознаванию 203 изображений ушей без окклюзий метод обеспечил правильное обнаружение во всех случаях. При тестировании метода в условиях окклюзии из 104 изображений, не участвовавших в обучающей выборке, удалось верно распознать только 54 примера. В работах [8, 9] исследователи также использовали AdaBoost для автоматического обнаружения уха на изображении.

Можно выделить следующие подходы к распознаванию ушной раковины [10].

- *Геометрический*. Методы из этой категории основаны на обнаружении границ внешнего уха. Как правило, информация о границах используется для описания геометрических свойств ушей или получения статистических данных, связанных с геометрией, которые можно использовать для распознавания;



*а* *б*

***Рис. 1. Обнаружение и нормализация ушной раковины 2D***

• *Целостный (структурный)*. Вычисляются некоторые характеристики изображения уха, такие, как коэффициенты Фурье, цветовые градиенты и т. д. Поскольку внешний вид уха значительно меняется с изменением позы или освещения, необходимо применять методы нормализации для коррекции этих изменений при извлечении признаков;

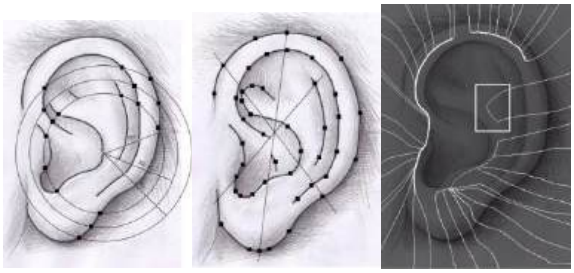
• *Локальный*. В отличие от геометрических подходов локальные подходы зависят не от расположения конкретных точек или отношений между ними, а от описания локальной окрестности (или области) некоторых точек на изображении. Точки, представляющие интерес для локальных подходов, не обязательно должны соответствовать конструктивно значимым частям уха, но в целом могут представлять любую точку на изображении. Такой подход чаще всего применяется при частичной окклюзии (сокрытии) ушей.

В качестве признаков (согласно системе Янарелли [11]) обычно выступают характерные точки структуры уха. Внешний вид наружного уха определяется формами завитка, противозавитка, козелка, противокозелка и других важных структурных частей (рис. 2, *а*).


*а* *б*

***Рис. 2. Наружное ухо:***
*а* — структура ушной раковины; *б* — ушной канал

Представление ушной раковины в зависимости от метода извлечения признаков может отличаться (рис. 3).



*а* *б* *в*

***Рис. 3. Примеры извлечения признаков разными методами:***
*а* — метод концентрических окружностей; *б* — метод активного контура; *в* — метод силовых полей

В научных работах находят применение следующие методы: концентрических окружностей (Concentric Circle Model, CCM) [12], активного контура (Active Contour Model, ACM) [13], силовых полей (Force Field Feature Extraction, FFFE) [14], главных компонент (Principal Component Analysis, PCA), масштабно-инвариантной трансформации признаков (Scale-Invariant Feature Transform, SIFT) [15], итеративный алгоритм ближайших точек и другие. В работе [9] для извлечения пространственных признаков различных направлений и масштабов применяется фильтр Габора (Gabor Filter). Признаки, извлеченные фильтром, имеют высокую размерность. Для снижения размерности применяется линейный дискриминантный анализ Фишера (Fisher's Linear Discriminant Analysis, FLDA). В табл. 1 представлены экспериментальные данные по 2D-распознаванию образов ушей на основе различных классификаторов и методов извлечения признаков.

Таблица 1

**Достигнутые результаты в области распознавания субъектов по двумерным изображениям ушей**

| Авторы | Метод извлечения признаков | Классификатор | База данных | Результаты |
|---|---|---|---|---|
| L. Yuan, Z. Mu [9] | Фильтр Габора | Модифицированный AdaBoost | 59 субъектов по 6 изображений, всего 354 изображения | EER = 4 % |
| D. J. Huley, M. S. Nixon, J. N. Carter [14] | Метод главных компонент + метод силовых линий | Расстояние Евклида, *k*-NN | 63 субъекта по 4 изображения, всего 252 изображения | EER = 13,5 % |
| A. Kumar, D. Zhang [16] | Логарифмический фильтр Габора (Log-Gabor Filter) | Расстояние Хемминга, *k*-NN | 113 субъектов, 265 изображений тренировочной выборки, 185 изображений тестовой выборки | EER = 10,5 % |
| I. Omara, X. Wu, H. Zhang [17] | Сверточные нейронные сети | Метод опорных векторов | 60 субъектов по 3 изображения, всего 180 изображений | EER = 4,2 % |
| E. Jeges, L. Mate [13] | Метод активного контура | Расстояние Хемминга, *k*-NN | 28 субъектов по 145 изображений, всего 4060 изображений | EER = 5,6 % |
| S. Prakash, P. Gupta [18] | Метод ускоренных надежных признаков (Speeded Up Robust Features, SURF) | Расстояние Евклида, *k*-NN | 300 субъектов по 7 изображений, всего 2066 изображений | EER = 2,5 % |

### Методы распознавания субъектов по трехмерному изображению уха

Трехмерные характеристики уха являются более информативными и могут предоставить более подробную информацию о глубине анатомической структуры уха [1]. Построение трехмерной модели уха может осуществляться двумя способами. Первый способ использует видеопоток как источник входных данных. Последовательная смена видеоизображений подразумевает изменение положения уха, а вместе с тем изменяется его ракурс, на основе которого получают трехмерную модель. Второй способ предполагает использование 3D-сканеров (рис. 4), стоимость которых лежит в пределах от 100 до 100000 долл. (в зависимости от разрешения и точности сканирования). Для задач распознавания образов уха вполне подойдут модели из нижнего ценового сегмента. Вычисление объема и формы объекта базируется либо на определении расстояния до него по времени возврата отраженных от его поверхности лучей, либо на стереоскопии (такие камеры имеют несколько объективов).


***Рис. 4. 3D-сканер Minolta VIVID 910***

При трехмерном распознавании анализируются аналогичные элементы уха (завиток, противозавиток и т. д. [19]), но при этом построение высокоточной 3D-модели ушной раковины дают гораздо больше информации. На рис. 5 показан результат сканирования поверхности ушной раковины 3D-сканером.

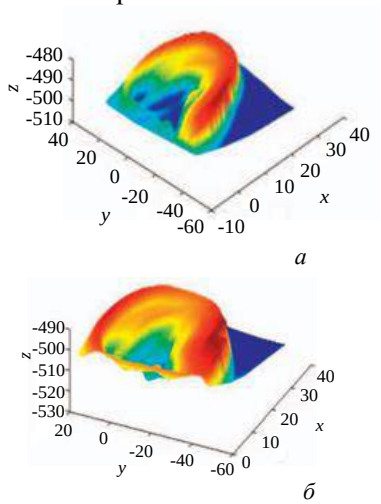
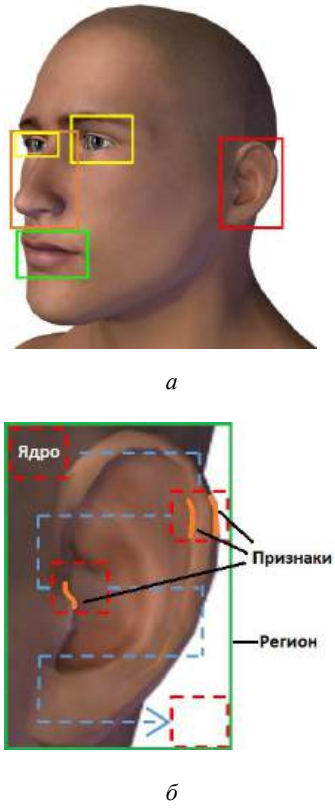



***Рис. 5. Пример 3D-изображения. На рисунках (а) и (б) показано два изображения одного уха, снятых с разных ракурсов (единицы измерения X, Y и Z — мм)***

Преимущество такого подхода в том, что трехмерная модель нечувствительна к освещению, а также к развороту и изменению ракурса (модель всегда можно повернуть в пространстве).

В исследовании [20] авторы предлагают гибридную систему распознавания ушной раковины на основе как локальных, так и целостных характеристик. Для обнаружения уха был использован алгоритм быстрых сверточных нейронных сетей (Faster Region-based Convolutional Neural Networks, Fast R-CNN) [21]. В данном алгоритме детектирование ушей происходит в два этапа. Первый этап основан на так называемой сети предложения регионов (Region Proposal Network, RPN), которая при помощи выборочного поиска (selective search) выделяет регионы, где может находиться ухо. Второй этап предполагает применение сверточной нейронной сети для поиска ушной раковины в предложенных регионах, что иллюстрирует рис. 6.




*а*

*б*

***Рис. 6. Принцип работы Faster R-CNN:***
*а* — RPN предлагает регионы; *б* — ядро CNN "скользит" по области, отвечает на вопрос: является ли предложенный регион ухом?

Извлечение локальных признаков в этой работе происходит с помощью дескриптора 3D-формы, основанного на гистограмме патчей поверхности индексированных фигур (Surface Patch Histogram Of Indexed Shapes, SPHIS). Целостные признаки извлекаются методом, предложенным в [22]. В табл. 2 представлены результаты экспериментальных данных нескольких работ по распознаванию трехмерных образов ушей.

Таблица 2

**Достигнутые результаты в области распознавания субъектов по параметрам трехмерных моделей ушей**

| Авторы | Метод извлечения признаков | Метод принятия решений | База данных | Результаты |
|---|---|---|---|---|
| H. Chen, B. Bhanu [19] | Локальное поверхностное исправление (Local Surface Patch, LSP) | Средняя квадратичная ошибка (Root Mean Square, RMS) | 302 субъекта, всего 942 изображения | EER = 2,3 % |
| Q. Zhu, Z. Mu [20] | SPHIS | Метод ближайших соседей | 500 субъектов по 4 изображения, всего 2000 изображений | EER = 2,2 % |
| P. Yan, K. Bowyer [4] | Собственный метод | Итеративный алгоритм ближайших точек (Iterative Closest Point, ICP) | 415 субъектов, всего 1386 изображений | EER = 1,2 % |
| S.M. Islam, R. Davies и др. [23] | Обнаружение ключевых точек (Key Point Detection, KPD) | Итеративный алгоритм ближайших точек | 415 субъектов по 2 изображения, всего 830 изображений | EER = 4,1 % |
| Y. Zhang, Z. Mu и др. [24] | Локальное изменение поверхности (Locale Surface Variation, LSV) | Итеративный алгоритм ближайших точек | 415 субъектов по 2 изображения, всего 830 изображений | EER = 2,3 % |

## Распознавание субъектов на основе акустических свойств уха

В отличие от оптических методов (2D, 3D) акустический метод требует прямого контакта для извлечения характеристик уха [5]. Метод может быть применен для разблокировки личных мобильных устройств, подтверждения аутентичности платежей или личности во время конфиденциальных переговоров.

Исследования показывают [5], что структура ушной раковины, длина и форма ушного канала (рис. 2, *б*) у людей очень различаются. Эти различия можно обнаружить при воздействии акустическими волнами на ушной канал с последующими измерениями отраженного сигнала. Спектр регистрируемого отраженного сигнала (или передаточной функции), содержащий информацию о геометрии ушного канала, может использоваться как вектор признаков. Работа [25] является одной из первых, где впервые описана идея построения вектора биометрических параметров на основе акустических свойств ушной раковины. Однако в ней отсутствуют данные о надежности предложенного подхода (EER, FRR, FAR).

Ушной канал вместе с ушной раковиной представляет собой резонансную систему (в грубом приближении это одномерная система, резонирующая на четверти длины акустической волны [5]), обладающую значительным идентификационным потенциалом, что обусловлено различием формы составляющих ее элементов и виброакустических свойств у разных людей. Длина слухового канала и кривизна ушной раковины имеют размеры, которые варьируются от миллиметров до нескольких сантиметров. Чтобы иметь возможность обнаруживать эти формы и кривые, акустические волны должны иметь надлежащие длины волн. Резонанс ушного канала в среднем составляет около 2500 Гц [5] и индивидуален у каждого человека.

При проектировании биометрической системы с использованием характеристик ушного канала необходимо учитывать тот факт, что стенки слухового прохода могут двигаться с движением челюсти. При этом формы изгибов в канале изменяются. Частотный диапазон для измерения отраженного сигнала может покрывать область от 1000 до 6000 Гц, где ухо обладает наибольшей возбудимостью. Низкие частоты не вызывают резонанса, поэтому их не анализируют. В зависимости от выбранного частотного диапазона меняется допустимый уровень звукового давления. Могут учитываться речевой (300—3400 Гц), музыкальный (27,5—4186 Гц) и ультразвуковой (свыше 20 кГц) диапазоны частот. Последний подход использовала компания NEC, представив в 2017 г. на выставке NEC EXPO наушники с функцией распознавания пользователя с точностью более 99 %. В представленной технологии от фирмы NEC используют ультразвуковые волны в диапазоне от 18 до 48 кГц, которые не слышны для пользователя и не вызывают дискомфорта. Сообщается, что технология усиливает безопасность за счет постоянного (непрерывного) распознавания, которое не мешает поведению или работе пользователей.

Принцип работы устройства для измерения акустических характеристик уха описан в работе [26] (рис. 7). Съем характеристик производится следующим образом: источник рядом с ушным каналом генерирует сигнал возбуждения, а приемник измеряет отраженные отклики. В общем случае возбуждение может представлять собой акустический сигнал, который имеет довольно плоский частотный спектр. Примерами устройств,

измеряющих акустические характеристики ушного прохода (раковины), могут служить внутриканальные и накладные наушники, либо мобильный телефон (при контакте с ухом).

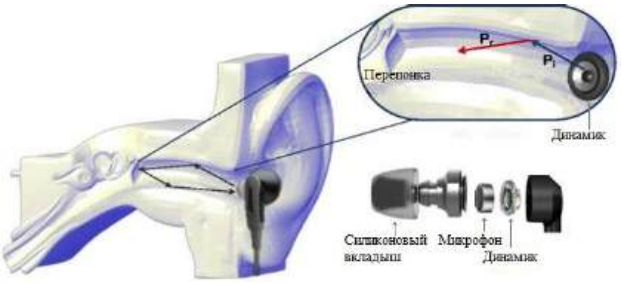



***Рис. 7. Принцип работы устройства для измерения акустических характеристик уха:***
звуковая волна транслируется в ушной канал ($P_i$), отражается от стенок раковины ($P_r$), микрофон регистрирует ответ

Ушной канал зондировали звуковыми волнами в диапазоне частот 1,5—2 кГц [5]. Вектор признаков включал по 256 значений на каждое ухо (всего 512 биометрических параметров). Признаки извлекали с использованием фильтра на основе метода перевалов (Method Of Steepest Descent). Для сравнения образов использовали средний уровень корреляций между векторами признаков (предъявленным и эталонным). Полученные показатели EER зависили от диапазона частот и используемого устройства и варьировались от 0,8 до 18 % (табл. 3).

Авторы работы [27] акустические характеристики уха использовали для генерации криптографических ключей. Данные характеристики регистрировали путем измерения передаточных функций от наушника к уху (headphone-to-ear-canal Transfer Functions, HpTF). Квантование данных производили нечетким экстрактором (Fuzzy Commitment) с применением метода главных компонент и случайного ортогонального преобразования. Размер вектора признаков составил 512 бит, по 256 бит для каждого уха. Сравнение образов производили методом ближайших соседей.

Проведено 2 эксперимента с привлечением 45 и 65 испытуемых (по 8 замеров на каждого) [27]. В первом случае наушники в течение всего эксперимента находились на испытуемых, во втором — наушники каждый раз снимали и надевали при каждом измерении. Монтаж динамика и микрофона существенно повлиял на вероятность ошибочных решений (табл. 3).

В сентябре 2019 г. команда исследователей [26] разработала прототип системы непрерывной биометрической аутентификации пользователей. Прототип получил название EarEcho. Он служит для подтверждения личности пользователя при ношении наушников. Процесс аутентификации EarEcho состоит из нескольких этапов: акустическое зондирование, предварительная обработка сигнала, извлечение признаков и аутентификация пользователя. На первом этапе динамиком излучается возрастающий ЛЧМ-сигнал (линейная частотная модуляция), охватывающий наиболее часто используемые звуковые полосы частот в диапазоне от 20 до 6 кГц, который распространяется через ушной канал, отражается и фиксируется микрофоном (рис. 8). Конструкция наушников выполнена таким образом, чтобы снизить помехи при излучении сигнала. Силиконовый вкладыш служит для шумоизоляции от внешней среды. На этапе предварительной обработки используется модуль контроля адаптивного усиления (Adaptive Gain Control, AGC), который подавляет нежелательные шумовые сегменты. Для исключения влияния сегментов с низким отношением сигнал/шум применяются тест отношения правдоподобия (Likelihood Ratio Test, LRT) и скрытые марковские модели. При помощи избирательного фильтра нижних частот отфильтровываются сигналы выше 6 кГц.

Взаимосвязь между излучаемым акустическим сигналом и записанным эхо-сигналом определяется особенностями строения внешнего уха и может быть смоделирована как не зависящая от времени линейная система, описываемая уравнением $Y(f) = H(f)X(f)$, где $X$ — сигнал на входе (моделируемый сигнал), $Y$ — записанный отраженный сигнал на выходе (после устранения шумов). Для системы с одним входом и одним выходом передаточная функция определяется как отношение спектральных плотностей мощности $X$ и $Y$ и может быть вычислена с помощью метода Уэлча. Основываясь на воспроизводимом (входном) сигнале и записанном

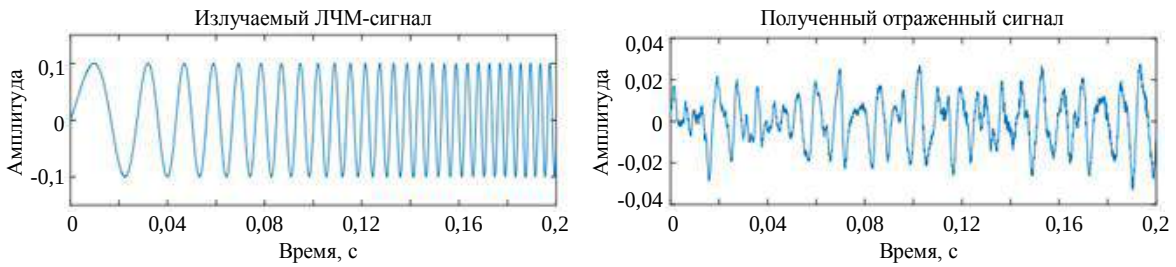



***Рис. 8. Посылаемый и полученный отраженный сигналы***

(выходном) эхо-сигнале, извлекают функцию с 2048 отсчетами дискретного преобразования Фурье и скользящим окном Ханна (длина окна 150 мс с перекрытием в 100 мс). Получается набор значений передаточных функций $G = \{H_1(f_1), H_1(f_2), \ldots, H_1(f_k)\}$, которые можно использовать как вектор признаков, где $H_1(f_k)$ — значение передаточной функции $k$-й полосы частот ($f_k < 6$ кГц). На рис. 9 показано 5 сигналов (2-минутных эпизодов разговора). Можно наблюдать, что извлеченные функции имеют высокую корреляцию и слабо зависят от контекста (входного сигнала) для одного и того же субъекта. При этом для разных субъектов передаточная функция существенно отличается.

В эксперименте приняло участие 20 испытуемых (возрастной диапазон 24—30 лет, 6 женщин и 14 мужчин). Во время сбора данных каждому субъекту было предложено надеть прототип наушников и прослушать 5 аудиозаписей длительностью в 2 мин. Участники снимали и надевали наушники между каждой аудиозаписью. Для имитации сценария ежедневного использования участники принимали разные позы (например, сидя и стоя). Данные собирали в различных условиях (при разном уровне шума, например комната, торговый центр, кафе, улица). Было собрано 11 900 образцов из 5 записей, каждый из которых представлял собой отрезок продолжительностью в 1 с. Образцы были разделены на две части: 80 % образцов отнесено к обучающей выборке, 20 % — к тестовой. Уровень звукового давления по умолчанию для обучения и тестирования составлял 55 дБ. При испытании использовали классификаторы ближайших соседей (K-Nearest Neighbor, k-NN), дерево принятия решений (Decision Tree, DT), наивный Байес (Naive Bayesian, NB), метод опорных векторов (Support Vector Machine, SVM), многослойный персептрон (Multi-layer Perceptron, MLP). В табл. 3 представлены результаты описанных исследований.

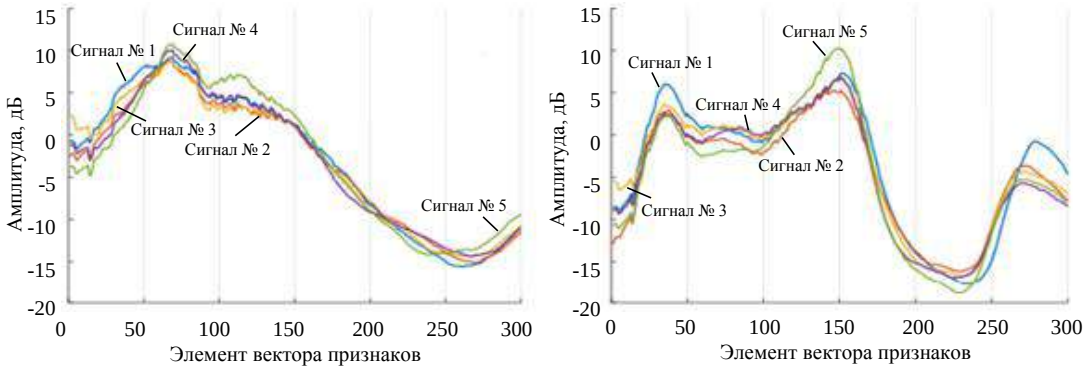



***Рис. 9. Усредненные векторы признаков двух пользователей при разных сигналах***

Таблица 3

**Достигнутые результаты в области распознавания субъектов по акустическим параметрам внешнего уха**

| Источник | Метод извлечения признаков | Метод принятия решений | База данных | | Результаты |
|---|---|---|---|---|---|
| T. Akermans, T. Kevenaar, D. Schobben [5] | Фильтр на основе метода перевалов | Сравнение среднего значения корреляции | Мобильный телефон: 17 субъектов по 8 замеров | | EER = 5,5—18 % |
| | | | Вставные наушники: 31 субъект по 8 замеров | | EER = 1—6 % |
| | | | Накладные наушники: 31 субъект по 8 замеров | | EER = 0,8—8 % |
| P. Tuyls, E. Verbitskiy, T. Ignatenko и др. [27] | Нечеткий экстрактор + метод $k$ ближайших соседей | | Эксперимент № 1 | 45 субъектов по 8 замеров | FRR = 0,8 %<br>FAR = 0,7 % |
| | | | Эксперимент № 2 | 65 субъектов по 8 замеров | FRR = 2,4 %<br>FAR = 4,4 % |
| Yang Gao, Wei Wang, Vir V. Phoha и др. [26] | Оконное преобразование Фурье | $k$-NN | 20 субъектов по 600 образцов, всего 11900 образцов | | FRR = 5—10 %<br>FAR = 7—15 % |
| | | DT | | | FRR = 9—15,2 %<br>FAR = 9—14,5 % |
| | | NB | | | FRR = 3—8 %<br>FAR = 9—27,5 % |
| | | MLP | | | FRR = 3—9,8 %<br>FAR = 4—8 % |
| | | SVM | | | FRR = 4—7 %<br>FAR = 3—7 % |

## Заключение

Преимущество методов распознавания личности человека по параметрам внешнего уха заключается в том, что этот тип образов скрыт от непосредственного наблюдения. У злоумышленника нет возможности создать достаточно информативную копию трехмерной модели внешнего уха скрыто от владельца или дистанционно. Наибольший интерес для исследователей и практических целей представляют методы идентификации и аутентификации личности по акустическим параметрам ушной раковины. Достигнутый уровень ошибочных решений распознавания личности по особенностям ушной раковины впечатляет (EER < < 0,8 %) [27].

Однако есть ряд нерешенных проблем. Требуется собрать базу данных параметров ушей большого объема для высокоточной оценки надежности (особенно FAR) методов идентификации и аутентификации по параметрам ушей. На данный момент имеющиеся базы составляют только несколько сотен образов (требуется несколько тысяч). Особенно это касается метода распознавания личности по акустическим характеристикам внешнего уха.

Известные исследования в основном направлены на разработку эффективных классификаторов, однако в реальной практике требуется создавать преобразователи "биометрия—код" на базе искусственных нейронных сетей (например, по ГОСТ Р 52633.5-2011). Таких исследований пока не проводилось.

Недостаточно глубоко исследован вопрос формирования зондирующих сигналов для "акустических" методов распознавания. Нет полноты данных о распределении частот резонанса ушного канала, а также об эффективности методов распознавания образов соответствующих передаточных функций при высоких частотах (более 20 кГц) зондирующих сигналов.

Тем не менее принципиальных проблем для построения высоконадежных систем распознавания личности на основе параметров внешнего уха выявлено не было.

*Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания в сфере научной деятельности (проект № 2.9314.2017/БЧ)*

**Литература**

1. *Pflug A., Busch C.* Ear biometrics: a survey of detection, feature extraction and recognition methods // IET biometrics. 2012. № 1(2). P. 114—129.

2. *Islam S., Bennamoun M., Owens R. A., Davies R.* A review of recent advances in 3D ear-and expression-invariant face biometrics // ACM Computing Surveys (CSUR). 2012. № 44 (3). P. 14.

3. *Yuan L., Mu Z. C., Yang F*A review of recent advances in ear recognition: Chinese Conference on Biometric Recognition. — Springer, Berlin, Heidelberg. 2011. P. 252—259.

4. *Yan P., Bowyer K. W.* Biometric recognition using 3D ear shape // IEEE Transactions on pattern analysis and machine intelligence. 2007. № 29 (8). P. 1297—1308.

5. *Akkermans T. H., Kevenaar T. A., Schobben D. W.* Acoustic ear recognition: International Conference on Biometrics. — Springer, Berlin, Heidelberg. 2006. P. 697—705.

6. *Emeršič Ž., Gabriel L. L., Štruc V., Peer P.* Convolutional encoder–decoder networks for pixel-wise ear detection and segmentation // IET Biometrics. 2018. № 7 (3). P. 175—184.

7. *Islam S. M., Bennamoun M., Davies R.* Fast and fully automatic ear detection using cascaded adaboost: In 2008 IEEE Workshop on Applications of Computer Vision. 2008. P. 1—6.

8. *Yuan L., Zhang F.* 2009, July. Ear detection based on improved adaboost algorithm: In 2009 International Conference on Machine Learning and Cybernetics. V. 4. P. 2414—2417.

9. *Yuan L., Mu Z.* Ear recognition based on Gabor features and KFDA // The Scientific World Journal. 2014. P. 12.

10. *Emeršič Ž., Štruc V., Peer P.* Ear recognition: More than a survey // Neurocomputing. 2017. 255. P. 26—39.

11. *Iannarelli A. V.* Forensic identification series: ear identification // Paramont Publishing Company, California. 1989. № 5. P. 213.

12. *Choraś M.* Perspective methods of human identification: ear biometrics. Opto-electronics review. 2008. № 16 (1). P. 85—96.

13. *Jeges E., Máté L.* Model-based human ear identification: In 2006 World Automation Congress. 2006, July. P. 1—6.

14. *Hurley D. J., Nixon M. S., Carter J. N.* Force field feature extraction for ear biometrics. Computer Vision and Image Understanding. 2005. № 98 (3). P. 491—512.

15. *Arbab-Zavar B., Nixon M. S., Hurley D. J.* September. On model-based analysis of ear biometrics: In 2007 First IEEE International Conference on Biometrics: Theory, Applications, and Systems. 2007. P. 1—5.

16. *Kumar A., Zhang D.* April. Ear authentication using Log-Gabor wavelets: Biometric Technology for Human Identification IV. 2007. V. 6539. P. 65390A. International Society for Optics and Photonics.

17. *Omara I., Wu X., Zhang H., Du Y., Zuo W.* Learning pairwise SVM on hierarchical deep features for ear recognition // IET Biometrics. 2018. № 7 (6). P. 557—566.

18. *Prakash S., Gupta P.* An efficient ear recognition technique invariant to illumination and pose // Telecommunication Systems. 2013. № 52 (3). P. 1435—1448.

19. *Chen H., Bhanu B.* Human ear recognition in 3D // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2007. № 29 (4). P. 718—737.

20. *Zhu Q., Mu Z.* Local and Holistic Feature Fusion for Occlusion-Robust 3D Ear Recognition // Symmetry. 2018. № 10 (11). P. 565.

21. *Ren S., He K., Girshick R., Sun J.* Faster R-CNN: Towards real-time object detection with region proposal networks: Advances in neural information processing systems. 2015. P. 91—99.

22. *Zhou J., Cadavid S., Abdel-Mottaleb M.* An efficient 3-D ear recognition system employing local and holistic features // IEEE transactions on Information Forensics and Security. 2012. № 7 (3). P. 978—991.

23. *Islam S. M., Davies R., Bennamoun M., Mian A. S.* Efficient detection and recognition of 3D ears // International Journal of Computer Vision. 2011. № 95 (1). P. 52—73.

24. *Zhang Y., Mu Z., Yuan L., Zeng H., Chen L.* 3D ear normalization and recognition based on local surface variation // Applied Sciences. 2017. № 7 (1). P. 104.

25. *Bouchard A. M., Osbourn G. C.* National Technology and Engineering Solutions of Sandia LLC, 1998. Systems and methods for biometric identification using the acoustic properties of the ear canal. U.S. Patent 5,787,187.

26. *Gao Y., Wang W., Phoha V. V., Sun W., Jin Z.* 2019. EarEcho: Using Ear Canal Echo for Wearable Authentication: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. № 3 (3). P. 81:1—81:24.

27. *Tuyls P. T., Verbitskiy E., Ignatenko T., Schobben D., Akkermans T. H.* August. Privacy-protected biometric templates: Acoustic ear identification: Biometric Technology for Human Identification. 2004, International Society for Optics and Photonics. 2004. V. 5404. P. 176—182.

# Personality recognition methods based on analysis of the characteristics of the outer ear

*(Review)*

*I. M. Garipov*
ITMO University, Saint Petersburg, Russia

*A. E. Sulavko, I. A. Kuprik*
Omsk State Technical University, Omsk, Russia

*The article describes approaches to extracting biometric parameters of the ear in two-dimensional and three-dimensional images, and the basis of measurements of the transfer functions of the ear canal. The methods used for pattern recognition for the construction of means of biometric identification and authentication according to the parameters of the auricle are considered. The main research results in this area are presented.*

*Keywords*: authentication, biometrics, personal identification, detection of the ear in the image, feature extraction, pattern recognition.

Bibliography — 27 references. *Received 19 December, 2019*

# ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004

## Безопасность распределенной автоматизированной системы

*Е. И. Митрушкин*, д-р техн. наук; *В. Р. Шавыкин*
АО «Ордена Трудового Красного Знамени научно-исследовательский институт автоматической аппаратуры им. академика В. С. Семенихина», Москва, Россия

*Предложена организация безопасности распределенной автоматизированной системы и ее составных частей.*

*Ключевые слова:* распределенная автоматизированная система, безопасность, комплексная система защиты, рубежи защиты.

### Типы и предметы угроз безопасности

Безопасность — это состояние защищенности автоматизированной системы (АС), ее составных частей и инфраструктуры от внешних и внутренних угроз. Безопасность крайне важна для государственной, военной и финансовой АС, иногда даже важнее ее функциональности.

Угроза безопасности автоматизированной системе — реально существующее или потенциально возможное событие, действие (воздействие), процесс, явление, условие, фактор или их совокупность, которые могут привести к нанесению ущерба АС, ее репутации, владельцам и пользователям, снижению эффективности, выводу из строя, уничтожению и даже действию АС в интересах конкурента или противника [1, 2]. К угрозам относятся:

- природные воздействия (землетрясения, извержения, наводнения, ураганы, молнии, пожары), а также агрессивность окружающей среды (температура, влага, вредные примеси в воздухе, насекомые, грызуны);
- техногенные аварии и катастрофы;
- непреднамеренные действия (воздействия) (отказы аппаратуры и инфраструктуры объектов автоматизации, ошибки и недостаточная квалификация обслуживающего персонала);
- преднамеренные действия (воздействия) обслуживающего персонала, конкурентов, противника, террористов, преступников и вандалов.

**Митрушкин Евгений Иванович**, профессор, ученый секретарь института.
E-mail: 89629785042@mail.ru
**Шавыкин Виктор Романович**, заместитель начальника отдела.
E-mail: 89629785042@mail.ru

*Статья поступила в редакцию 27 января 2020 г.*



Предметами воздействия угроз могут быть АС в целом, объекты автоматизации и инфраструктура, персонал, аппаратура и коммуникации, программы, информация.

Виды угроз и предметов их воздействия приведены на рис. 1.

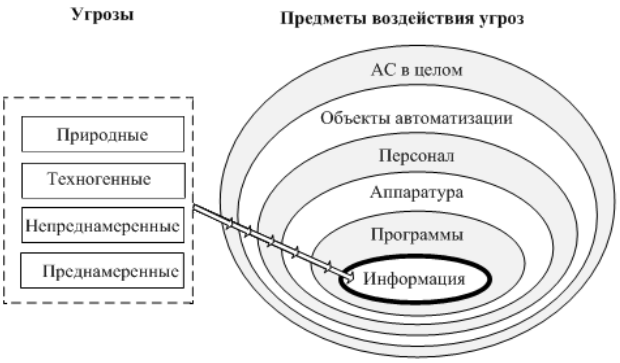



***Рис. 1. Виды и предметы угроз безопасности АС***

Угрозы могут нарушать безопасность АС в случае наличия у нее уязвимости — свойства (недостатков), обуславливающего возможность реализации угроз [2, 3].

### Комплексная система защиты АС

Для минимизации угроз и устранения последствий их воздействия необходима комплексная система защиты АС (или комплексная система обеспечения безопасности АС).

На рис. 2 представлена обобщенная схема обеспечения безопасности АС.

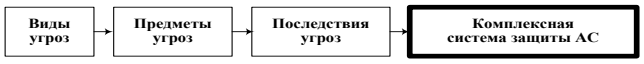



***Рис. 2. Обобщенная схема обеспечения безопасности АС***

Она предусматривает безусловную реализацию совокупности мероприятий, решений и средств защиты на всех стадиях жизненного цикла АС, в том числе:

- законодательные и правовые документы (государственные, ведомственные и корпоративные), предусматривающие уголовную или административную ответственность должностных и посторонних лиц;
- организационные и режимные мероприятия, затрудняющие разведывательную, террористическую и противоправную деятельность;
- инженерные и технические решения, методы и средства защиты от всех угроз.

Возможна также страховая форма защиты.

Процесс создания комплексной системы защиты АС включает в себя ряд мероприятий и работ, которые представлены в табл. 1.

Таблица 1

**Этапы создания и технической поддержки комплексной системы защиты АС**

| Этапы работ | Мероприятия и работы, выполняемые на данном этапе | Разрабатываемые документы |
|---|---|---|
| 1 | Проведение обследования АС и анализ источников угроз, оценка уязвимостей и рисков, создание модели нарушителя | Протоколы обследования,<br>модель нарушителя,<br>акты и т. д. |
| 2 | Разработка концепции защиты АС на основе обследования и анализа источника угроз, оценки уязвимостей и рисков и модели нарушителя | Концепция защиты |
| 3 | Разработка политики безопасности и комплекса мер по ее реализации на основе концепции защиты | Политика безопасности |
| 4 | Разработка (уточнение) требований по защите отдельных технических средств и программного обеспечения, а также для системы защиты информации объекта АС в целом | Требования по защите информации,<br>схема функционирования,<br>состав средств защиты и т. д. |
| 5 | Выбор (уточнение) средств защиты (аппаратных, аппаратно-программных, программных и криптографических) для построения системы комплексной защиты информации | Договора на закупку средств защиты информации (АПМДЗ, САВЗ, МЭ и т. д.) |
| 6 | Разработка тестов контроля и оценки эффективности системы защиты информации АС | Тесты контроля |
| 7 | Разработка эксплуатационной документации в соответствии с ГОСТ Р 50739-95 | Руководство пользователя,<br>руководство по системе защиты,<br>тестовая документация,<br>конструкторская (проектная) документация |
| 8 | Установка средств защиты и настройка функционирования системы защиты информации в АС, проведение испытаний (предварительных и государственных) для присвоения документации литеры "$О_1$" | Протоколы испытаний,<br>акты, решения, заключения и т. д. |
| 9 | Подготовка организационных документов и совместное участие с сертификационной лабораторией в проведении сертификации средств защиты и системы защиты информации АС в целом | Формирование заявки и перечня сведений об АС и КСЗ на проведение сертификации с указанием класса защищенности АС;<br>получение решения от органа по сертификации для заключения договора с сертификационной лабораторией;<br>разработка ТЗ на проведение работ по сертификации АС;<br>заключение договора с лабораторией сертификации;<br>согласование Программы и методик проведения сертификации;<br>получение протоколов от лаборатории,<br>получение технического заключения и сертификата соответствия по требованиям безопасности информации от органа сертификации |
| 10 | Сопровождение и техническая поддержка функционирования средств защиты и системы защиты информации АС | Протоколы авторского надзора, акты и т. д.;<br>заявки на проведение сертификации или инспекционного контроля в случае замены ОС, доработок или изменений, внесенных в ПО, СПО АС |

**Рубежи защиты АС**

Комплексная система защиты АС может предусматривать несколько рубежей защиты (защитных оболочек, периметров защиты, уровней защиты). Их виды и количество определяются спецификой конкретной АС. В качестве примера рассмотрим шесть рубежей защиты (в соответствии с рис. 1).

**1-й рубеж —** *защита АС в целом*:

- маскировка и легендирование АС, работ и средств;
- разработка перечня и грифа охраняемых сведений и средств, инструкций по безопасности для каждой стадии жизненного цикла АС;
- создание необходимых условий для проведения работ и совещаний с закрытой информацией.

**2-й рубеж** — *защита объектов автоматизации и инфраструктуры*:

- физическая, химическая и другие виды защиты территорий, зданий, помещений и инфраструктуры;
- ограждение, охрана и оборона сооружений, обеспечение видеонаблюдения и контролируемой зоны, запрет автостоянок;
- аттестация объектов автоматизации по требованиям безопасности; специальные исследования и проверки объектов;
- экстренное уничтожение объекта (при попытке его захвата).

**3-й рубеж** — *защита персонала* (обеспечение кадровой безопасности или кадрового режима):

- отбор, обучение и постоянная проверка персонала АС;
- привлечение к работам сотрудников, имеющих допуск, и организаций, имеющих соответствующие лицензии, доведение до них только их касающихся сведений.

**4-й рубеж** — *защита аппаратуры автоматизации, телекоммуникации и связи*:

- обеспечение стойкости к природным, механическим, климатическим, биологическим, специальным и иным воздействиям;
- использование бесперебойного электропитания;
- снижение потребления и излучения энергии, выбор оптимальных спектров излучения;
- снижение побочных электромагнитных излучений и наводок сигналов (экранирование и зашумление аппаратуры, линий и кабелей) для противодействия техническим разведкам;
- защита, контроль и регистрация доступа к аппаратуре, линиям, кабелям и инфраструктуре (электромеханические замки и ключи, датчики и пульты доступа, вскрытия или отключения аппаратуры);
- сертификация аппаратных средств и средств защиты;
- экстренный подрыв (уничтожение) аппаратуры и линий.

**5-й рубеж** — *защита программ*:

- сертификация программных средств по требованиям безопасности;
- применение средств доверенной загрузки программ;
- разграничение, контроль и регистрация доступа к защищаемым программным ресурсам;
- антивирусная защита программ;
- экстренное стирание (уничтожение) программ и носителей.

**6-й рубеж** — *защита информации*. Этот рубеж защиты обеспечивает ряд свойств безопасности информации:

- целостность информации — состояние информации, при котором обеспечивается достижение целей ее функционального применения в системе в условиях случайного и/или преднамеренного искажения (разрушения);
- конфиденциальность информации — свойство используемой информации быть сохраненной в течение заданного периода конфиденциальности от ознакомления лицами, к ней не допущенными, и/или от несанкционированного считывания техническими средствами;
- секретность информации, составляющей государственную тайну;
- доступность информации — состояние информации, ее носителей и технологий обработки, при котором обеспечивается надежный, своевременный и санкционированный доступ к ней.

Термины "информация" и ее "безопасность" используются в двух сочетаниях, имеющих разный смысл.

*Информационная безопасность* (ИБ) — состояние защищенности информационной среды общества, интересов граждан, организаций и государства, при котором исключаются воздействия, угрожающие их существованию. Информационная безопасность связана с воздействием на сознание, с безопасным функционированием умов. Таким образом, объектом защищенности являются граждане, организации, общество и государство.

*Безопасность информации* (БИ) — состояние защищенности автоматизированной системы (АС), ее составных частей и инфраструктуры от внешних и внутренних угроз и уязвимостей. Таким образом, объектом защищенности является информация. Данный термин является предметом рассмотрения.

### Комплексная система защиты информации

Разные уровни распределенной АС используют собственные виды информации, некоторые из которых приведены в табл. 2.

В зависимости от назначения АС эта информация подразделяется на открытую информацию, конфиденциальную информацию, в отношении которой обладателем введен режим коммерческой или корпоративной тайны, и информацию, отнесенную к государственной тайне и имеющую соответствующий гриф секретности [4].

Таблица 2

**Уровни и виды информации распределенной АС**

| Уровень информации | Виды информации | | |
|---|---|---|---|
| | целевая | контроля функционирования | обеспечения безопасности |
| Общесистемная информация, циркулирующая между объектами автоматизации | Приказы, подтверждения и донесения, распоряжения и указания, системные базы данных, электронная почта, документооборот, отчеты и справочная информация | Информация о состоянии объектов автоматизации и их комплексов | Сообщения о несанкционированных действиях (НСД) на объектах автоматизации<br>Приказы блокировки функционирования объекта автоматизации или его комплекса |
| Внутриобъектовая информация, циркулирующая только внутри одного конкретного объекта автоматизации | Базы данных объекта, его электронная почта, внутренний документооборот и справочная информация | Информация о состоянии собственных комплексов, а также о состоянии подчиненных и взаимодействующих объектов автоматизации и их комплексов | Информация системы разграничения доступа пользователей к ресурсам объекта автоматизации |
| Информация, циркулирующая только внутри одного конкретного комплекса объекта автоматизации | Локальные базы данных, внутренняя электронная почта, справки | Информация о состоянии комплекса и взаимодействующих комплексов объекта автоматизации | Информация многофакторной идентификации и аутентификации пользователей, системы контроля и разграничения доступа |

Вариант обобщенной схемы обеспечения безопасности информации приведен на рис. 3.

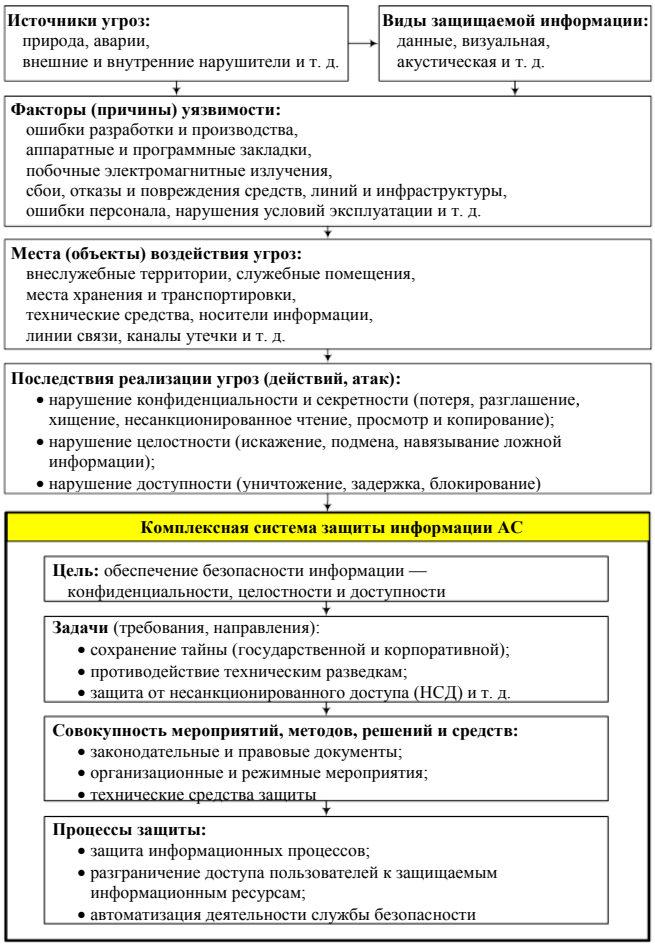



***Рис. 3. Обобщенная схема обеспечения безопасности информации***

На рис. 3 выделена комплексная система защиты информации (КСЗИ), обеспечивающая минимизацию угроз и последствий их воздействия на защищаемую информацию АС. КСЗИ позволяет обрабатывать информацию с требуемым уровнем защищенности и выполнять требования по защите информации от утечки, разглашения, несанкционированного доступа и воздействия, непреднамеренного и преднамеренного воздействия, действий сторонней технической разведки.

Процессы защиты КСЗИ можно объединить в три большие группы (см. рис. 3).

1. **Защита информационных процессов**.

- Резервирование (дублирование) информационных процессов в рассредоточенных средствах и даже объектах автоматизации (обеспечение отказо- и катастрофоустойчивости информации).
- Криптозащита (шифрование) информации для скрытия ее содержания (в том числе на внешних носителях). Общая схема шифрования передаваемой информации приведена на рис. 4.

В зависимости от специфики АС и ее телекоммуникационной сети (сетей) используют линейное шифрование (в линиях сети), абонентское шифрование (на рабочих местах пользователей объектов автоматизации), а также их сочетания [5] (рис. 5).

Все типы шифрования являются своеобразным флагом и делают информацию подозрительной для заинтересованных лиц — противника, конкурента, властей.

- Стеганография (стеганозащита) для сохранения в тайне (скрытия) самого факта наличия или передачи защищаемой информации.
- Имитозащита для обеспечения подлинности информации и отправителя, противодействия навязыванию ложной информации (дезинформации) противником или злоумышленником.

Применяются электронная подпись, открытые ключи, процедуры аутентификации, контроль времени приема сообщения относительно момента выдачи его в сеть (протоколами канального, сетевого и представительского уровней) и т. д.

- Антивирусная защита информации, направленная на запрет доступа незарегистрированных программ, процессов, файлов и т. д.

Используется антивирусный контроль съемных носителей информации, а также контроль перед загрузкой или перезагрузкой программного обеспечения, при сбоях вычислительного процесса, когда неизвестна причина сбоя, после завершения регламентных и профилактических работ.

- Межсетевое экранирование для безопасного обмена информацией (данными) между комплексами и сетями. Межсетевой экран (МЭ) представляет собой локальное или функционально распределенное средство (комплекс), устанавливаемое, как правило, на границах внутренних и внешних сетей или разных комплексов. МЭ контролирует (фильтрует) проходящую информацию в соответствии с заданными критериями и правилами обеспечения безопасности конкретного объекта автоматизации или АС в целом.
- Автоматическая регистрация и документирование (при необходимости) информации, учет документооборота.

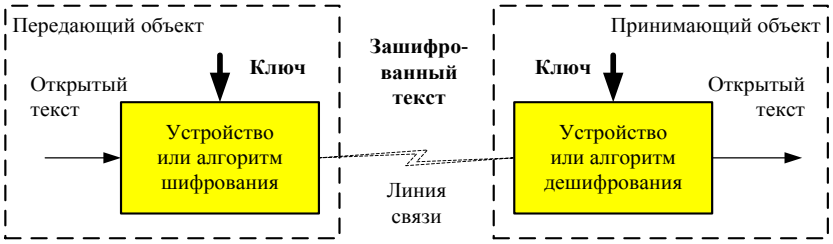



***Рис. 4. Шифрование и дешифрование передаваемой информации***

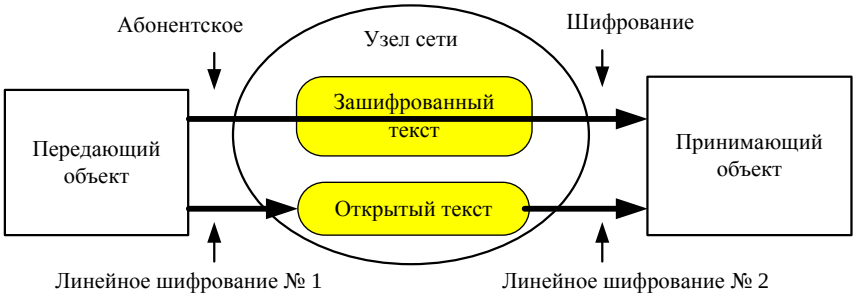



***Рис. 5. Организация линейного и абонентского шифрования***

Вся входящая и исходящая информация автоматически регистрируется с проставлением атрибутов: регистрационный номер сообщения; дата регистрации (число, месяц, год); внешний адрес отправителя; внутренний адрес получателя; уровень конфиденциальности или секретности (мандатная метка сообщения) и т. д.

Документирование информации производится на учтенном бумажном носителе с автоматически проставляемыми соответствующими атрибутами и с обязательной регистрацией в журнале распечаток, который хранится в отдельной области памяти автоматизированного рабочего места (АРМ) администратора безопасности.

- Хранение документов и съемных носителей в противопожарных сейфах.

2. **Разграничение доступа пользователей к защищаемым информационным ресурсам** с учетом их степени важности и формы допуска пользователя.

- Многофакторная идентификация и аутентификация пользователей. Могут быть использованы многоуровневые аппаратные и программные ключи, а также биометрические параметры.
- Использование многомерной матрицы разграничения доступа.

Для разграничения доступа пользователя к информации, хранимой в другом комплексе объекта автоматизации, используется межсетевой экран.

- Автоматический контроль и регистрация доступа пользователей к защищаемой информации.
- Исключение доступа представителей службы эксплуатации к защищаемой информации.

3. **Автоматизация деятельности службы безопасности** для управления средствами и процессами защиты информации: своевременного контроля нарушения защитных рубежей, сохранности и целостности информации и действий пользователей; оперативного принятия решений по предотвращению несанкционированного доступа (НСД) пользователей к защищаемым информационным ресурсам и по ликвидации последствий НСД.

- Применение выделенного АРМ администратора безопасности объекта.
- Автоматическая сигнализация и регистрация всех фактов и попыток доступа, вскрытия, подключения или отключения защищаемых ресурсов: аппаратуры, кабелей, рабочих помещений и кузовов-фургонов; сигнализация о каждой попытке НСД и отключении средств регистрации; документирование информации и т. д.
- Внутриобъектовый контроль и администрирование рубежей и средств защиты, действий пользователей и защита от НСД в объекте автоматизации:

– контроль применения на АРМ пользователей средств разблокировки, а также соблюдение пользователями правил разграничения доступа;

– блокировка работы пользователя при возникновении НСД (путем блокировки конкретного АРМ и даже конкретного комплекса в целом);

– оперативное восстановление функций КСЗИ после сбоев за счет ведения двух копий специальных программных средств и их периодического обновления;

– периодическое тестирование всех функций КСЗИ с помощью специальных программных средств не реже одного раза в неделю.

- Централизованный контроль уполномоченным лицом на управляющем объекте распределенной АС выполнения пользователями правил работы в системе с защищаемыми информационными ресурсами и защита от НСД в системе:

– контроль достоверности информации и действий всех пользователей распределенной АС (контроль применения на объектах автоматизации средств разблокировки);

– автоматическая выдача и доведение до вышестоящего объекта соответствующих сообщений при возникновении НСД или навязывании ложной информации на любом объекте автоматизации;

– блокирование функционирования этого объекта автоматизации или его конкретного комплекса путем выдачи соответствующего сообщения с вышестоящего объекта АС.

Организация контроля действий пользователей на объекте автоматизации и в системе проиллюстрирована на рис. 6.


***Рис. 6. Организация контроля и блокировки действий пользователей***

- Экстренное стирание (уничтожение) информации при угрозе захвата объекта автоматизации, возникновении НСД или сдаче аппаратуры в ремонт или утилизацию.

### Выводы

Предложенная структуризация отражает оптимальную организацию защиты распределенной автоматизированной системы.

Предложенные рубежи защиты в значительной степени позволяют обеспечить конфиденциальность, секретность, целостность и доступность информации в любой автоматизированной системе.

Решения по безопасности должны постоянно совершенствоваться, иначе победа достанется конкуренту или противнику.

**Литература**


1. ГОСТ Р 50922–2006 Защита информации. Основные термины и определения.
2. *Митрушкин Е. И.* Системотехника. Инженерные основы автоматизированных систем: учеб. пособие. — М.: Московский государственный институт радиотехники, электроники и автоматики (технический университет), 2013. — 200 с.
3. ГОСТ Р 56545–2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей.
4. *Митрушкин Е. И., Шавыкин В. Р.* Рубежи защиты автоматизированной системы: тр. 21-й Международной научно-технической конф. "Современные телевидение и радиоэлектроника". 19–20 марта 2013 г., Москва. — М.: ФГУП МКБ "Электрон", 2012. С. 295—299.
5. *Митрушкин Е. И., Шавыкин В. Р.* Защита информации в распределенной автоматизированной системе: тр. XII Российской научно-технической конф. "Новые информационные технологии в системах связи и управления". — Калуга, 5 июня 2013 г. — Калуга: Изд-во ООО "Ноосфера", 2013. С. 54—59.


## Security of a distributed automated system


*E. I. Mitrushkin, V. R. Shavykin*
Stock Company "Research Institute for Automated Apparatus named after academician V. S. Semenikhin", Moscow, Russia



*The security organization of a distributed automated system and its components is proposed.*



*Keywords*: distributed automated system, security, complex protection system, frontiers of protection.

Bibliography — 5 references. *Received January 27, 2020*

УДК 004.056

# Способы привлечения руководящего состава к выработке политики безопасности корпоративных сетей

*А. С. Вилков*; *М. М. Тараскин*, д-р техн. наук
Войсковая часть № 11928, Москва, Россия

*Рассматриваются способы привлечения руководящего состава организаций к мероприятиям по созданию комплексной безопасности. Одним из важных направлений в данном процессе является выработка политики безопасности корпоративных сетей. Рассматривается совокупность пошаговых мероприятий, направленных на формирование политики безопасности в организации, в частности корпоративных сетей. В материалах рассматриваются с той или иной степенью детализации мероприятия в областях нормативных, организационных, а также аппаратно-программных. В выводах представлены конкретные рекомендации по преодолению пассивного отношения руководящего состава организаций к мероприятиям по созданию комплексной безопасности. Приведены руководящие документы (РД) ФСТЭК России, относящиеся к рассматриваемой проблеме.*

*Ключевые слова:* политика безопасности корпоративных сетей, информационная безопасность, угрозы, уязвимости и риски, информация, защита информации.

## О политике информационной безопасности

Политика информационной безопасности является планом высокого уровня, в котором описываются цели и задачи мероприятий в сфере безопасности. Политика не представляет собой ни директиву, ни норматив, ни инструкции, ни средства управления. Политика описывает безопасность в обобщенных терминах без специфических деталей. Она обеспечивает планирование всей программы безопасности так же, как спецификация определяет номенклатуру выпускаемой продукции [1].

Когда заявляют, что технологический процесс не является частью политики, всегда появляются вопросы. Технологический процесс представляет собой детальное описание всех действий. Политика представляет собой изложение целей, которые должны быть достигнуты внедрением этого технологического процесса. Для описания политики используют общие термины, так что политика не оперирует способами реализации. Например, если политика определяет единственное решение производителя для единственного контракта, то в компании возникают трудности, когда появляется необходимость модернизации для создания новой продукции. Несмотря на то что при разработке политики может потребоваться технологическая документация, сама технологическая документация не должна являться частью политики [2].

## Почему важно работать по правилам информационной безопасности

Несмотря на то что политика не отвечает на вопрос, каким образом должны достигаться технологические цели, определив должным образом, что необходимо обезопасить, мы тем самым обеспечиваем надлежащее управление процессом. В правилах безопасности описано, что должно быть защищено и какие ограничения накладываются на управление. В них не обсуждается ни номенклатура производимого продукта, ни производственные циклы, но правила безопасности помогают лучше ориентироваться и при выборе продукта, и при выборе путей развития компании. Реализация требований политики обеспечит более высокую защищенность всей системы.

Если в разработке политики информационной безопасности принимает участие руководство, это свидетельствует о том, что руководство приветствует идею создания политики безопасности, наделяя доверием всю программу безопасности. Поддержка руководства всегда важна, без нее служащие не станут воспринимать политику серьезно. Поэтому без поддержки вышестоящего руководства программа внедрения политики безопасности обречена на неудачу еще до окончания ее разработки [2].

Руководство может заявить, что каждый должен нести ответственность за безопасность на своем участке работы. Такой подход может иметь успех, но только короткий период времени, пото-

**Вилков Андрей Сергеевич**, старший преподаватель.
E-mail: rubico@mail.ru
**Тараскин Михаил Михайлович**, сотрудник.
E-mail: rubico@mail.ru

*Статья поступила в редакцию 26 января 2020 г.*

му что при этом не происходит развития компании. Если один отдел использует один стандарт, а другой отдел использует другой, то возможность их взаимодействия становится проблематичной. Работа по единым правилам гарантирует, что в организации используют одни и те же стандарты, когда дело касается безопасности. Такая слаженность дает возможность работать организации как единому механизму, облегчает взаимоотношения с клиентами и поднимает значение информационной защиты всей системы [1].

И наконец, политика информационной безопасности поможет наладить четкую работу. Если пытаться внедрять правила, которые не сформулированы четко, то нужно быть готовым к судебным разбирательствам. Если вы решите уволить служащего за нарушение правил безопасности, которые никогда не существовали в письменном виде, не были вручены служащему, то этот служащий может подать в суд на компанию [3].

### Когда необходимо иметь разработанные правила безопасности

Лучше всего разработать правила еще до того, как появится первая проблема с безопасностью. Если осуществить это заранее, то администраторы безопасности будут понимать, что именно необходимо защищать и какие меры нужно предпринимать. Кроме того, всегда легче разработать политику для развивающейся инфраструктуры, чем пытаться модифицировать уже существующий режим экономической деятельности.

### Уменьшение степени риска

Бизнес невозможен без риска. Для уменьшения степени риска принимают меры предосторожности. При разработке политики безопасности анализируют бизнес-процессы и применяют лучшие методы для обеспечения их защиты. Это также может уменьшить потери, понесенные компанией, в случае утери важной информации [3].

Информационная безопасность и защита компьютеров от вирусов стали неотъемлемой частью служб безопасности. Правовые органы серьезно взялись за борьбу с преступлениями в сфере электронной обработки информации. Все больше дел поступает в суды, чтобы распространить действующие законы на совершенно новый вид преступлений, совершенных в электронном мире. Компании, не имеющие четко разработанных правил, обнаружили, что им трудно выяснять отношения в суде, так как суд рассматривает только четкие формулировки. Компании, которые разработали четкие правила безопасности еще до того, как им пришлось столкнуться с необходимостью защищать свои права в суде, имеют несомненное преимущество.

Новая экономика предусматривает страховые надбавки на электронную информацию. Электронная информация и компьютеры, на которых она обрабатывается, стали неотъемлемой частью бизнеса, поэтому компании стремятся застраховать эти активы. В свою очередь, страховые компании интересуются политикой безопасности и методами ее реализации компаниями. Первый вопрос, который Вам зададут при заключении договора страхования, будет касаться именно политики безопасности. Страховым компаниям известно, что без разработанной политики безопасности компания не знает степень защищенности своих активов и, соответственно, страховать операции таких компаний рискованно [2].

Политика безопасности, в которую включены методики разработки программного обеспечения, будет стимулировать разработку более защищенных систем. Руководствуясь такими принципами и стандартами, разработчик сможет работать согласно установленным нормативам, испытатели систем будут знать, какие результаты должны быть получены, а администраторы будут понимать, что требуется от конкретного технологического процесса. Развитие компании по индивидуальному проекту всегда требует больших материальных затрат и ответственного отношения к работе. Путем разработки и внедрения правил разработки программного обеспечения, а также предоставления разработчикам нормативов разработки риск в бизнесе может быть значительно уменьшен [4].

### После прорыва защиты

После прорыва защиты внедрение установок политики безопасности остается необходимым, поскольку один раз это уже произошло, вполне может произойти снова [2].

Приступая к разработке политики безопасности после того, как защита взломана, не нужно фокусировать внимание только на той части системы, в которой был прорыв защиты, однако эту часть системы нужно учесть в разработке, ее нужно рассматривать как одну из многих критичных с точки зрения защиты частей. Необходимо всегда рассматривать проблему в целом и никогда не фокусировать внимание на отдельной детали.

### Соответствие документации

Правительственные чиновники, подрядчики государственных заказов, т. е. те, кто нанят под-

рядчиками для выполнения государственных заказов, и сотрудники прочих предприятий, работающие в государственном секторе экономики, должны обеспечивать надежную и безопасную работу систем на своих предприятиях.

Правительство и другие заказчики испытывают все большую потребность в четко определенных правилах информационной безопасности. Даже в самом начале нового проекта наличие наработок в области политики безопасности демонстрирует заказчику, что он имеет дело с серьезным партнером, способным обеспечить защиту и своих информационных активов, и активов заказчика.

Первой заботой компании должно быть наличие политики безопасности, начиная с заключения соглашения и выполнения правовых норм и заканчивая претворением проекта в жизнь.

### Демонстрация усилий по управлению качеством

Компании демонстрируют заказчику, что их технологии соответствуют стандартам управления качеством продукции. Международная организация по стандартизации (InternationalStandardsOrganization — ISO) 9001 описывает стандарты управления качеством в технологических и бизнес-процессах. Если компания хочет получить определенный уровень аккредитации, ее политика направлена на внедрение программы безопасности, отвечающей установленным стандартам управления качеством [5].

### Каким образом нужно разрабатывать правила безопасности

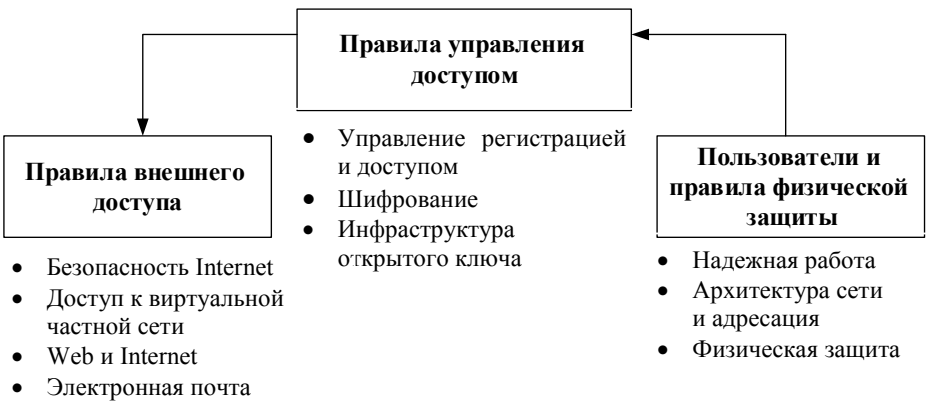
Прежде чем приступать к разработке руководящих документов, необходимо определить глобальные цели политики: заключается цель в защите компании и ее взаимодействия с клиентами или необходимо обеспечить защиту потока данных в системе? В любом случае на первом этапе необходимо определить, что нужно защищать и почему именно это должно быть защищено [2].

Правила могут быть написаны для защиты аппаратных средств, программного обеспечения, средств доступа к информации, людей, внутренних коммуникаций, сети, телекоммуникаций, правоприменения и т. п. Перед тем как начинать процесс разработки правил, нужно определить, какие системы и технологические процессы являются важными для выполнения задач компании. Это поможет определить, сколько и каких правил должно быть разработано для успешной деятельности компании.

### Определите, какие правила необходимо разработать

Правила информационной безопасности не должны быть единым документом. Чтобы упростить пользование ими, правила могут быть включены в несколько документов. Нет необходимости описывать политику компании одним документом. Небольшие разделы легче понимать, легче внедрять и проще организовать, корректировать и обновлять [2].

Для каждой системы, обеспечивающей бизнес, и каждой подзадачи, на которые может быть разбита глобальная цель бизнеса, необходимо разработать отдельный документ. Нормально разрабатывать антивирусную защиту отдельно от правил использования Internet. Общепринятая ошибка заключается в попытках слить описание политики безопасности в один документ, который обрисовывает только общие принципы. В результате появляется обширный документ, с которым очень трудно работать, который, возможно, никогда не будет прочитан и не получит никакой поддержки. На рисунке представлен примерный перечень систем, для которых разрабатываются правила информационной безопасности [2].




***Примерный перечень систем, поддерживающих бизнес, для которых разрабатываются правила информационной безопасности***

Накоплена масса доказательств того, что человек не в состоянии сосредоточить внимание на чем-то одном длительное время. Правила информационной безопасности не являются исключением [5]. Сжатое изложение правил с ясными формулировками и логическим обоснованием в четко скомпонованном документе даст шанс этому документу быть прочитанным.

### Оценка риска. Анализ или аудит

Способ понять инфраструктуру заключается в полной оценке риска, анализе рисковых ситуаций или полном аудите предприятия. Выполнив все это, разработчики основ политики безопасности смогут хорошо разобраться в информационных технологиях организации. Эта работа помогает авторам документов политики всесторонне понять архитектуру системы.

Для оценки степени риска организация может провести тестирование на преодоление защиты. Это тестирование должно быть выполнено во внутренней и внешней сети, чтобы проверить каждую точку доступа и выявить неизвестные точки доступа. Такая всесторонняя оценка позволит вникнуть в конфигурацию сети. Эта информация будет использована для определения конфигурации, правил доступа в сеть и других правил. Кроме того, такая оценка выявит, насколько сеть обеспечивает выполнение задач организации.

Некоторые администраторы полагают, что исследовать систему, определить степень риска и провести инвентаризацию предприятия можно без посторонней помощи. Несмотря на то что администраторы могут выполнить соответствующую работу, всегда лучше пригласить для нее кого-то со стороны. Сторонние представители могут выявить уязвимые места, слабости защиты и другие проблемы, которые следует учесть при разработке правил информационной безопасности [2].

### Критическая оценка, утверждение и претворение в жизнь

Любой корпоративный документ обычно подвергается критической оценке. Правила информационной безопасности — это документы, различные по содержанию. В процессе рецензирования должны рассматриваться не только технические аспекты безопасности, но и юридические аспекты, поскольку это имеет непосредственное отношение к организации. До начала разработки правил любого уровня должно быть проведено детальное обследование объекта. Предварительное обследование должно быть выполнено разработчиками правил безопасности, и лишь после этого должно выполняться обследование на более низких уровнях. Если в компании есть CIO (ChiefInformation-Officer — руководитель информационной службы компании), то он должен быть в составе комиссии по обследованию объекта. Руководители департаментов или руководители отделов, которые будут иметь непосредственное отношение к разработке правил, также могут участвовать в рецензировании и делать комментарии, юристы корпорации также должны принимать в этом участие. Юристы понимают раздел правил безопасности, касающийся правоприменения, и знают, каким образом придать правилам законную силу.

Процесс утверждения представляет собой простое одобрение руководством окончательной версии документа. Их утверждение должно состояться после рецензирования. Если руководство не одобрит эти документы, их эффективность будет ограничена.

После того как правила будут написаны, утверждены и администраторы получат необходимые инструкции, политика начнет претворяться в жизнь. Если отдельные правила не будут приведены в исполнение, это нарушит целостность всей политики [2].

### Предварительные выводы

*Правила, составляющие политику безопасности:*

- не заменяют инструкции и стандарты;
- не являются производственными директивами и средствами управления;
- описывают безопасность в общих терминах и не описывают, каким образом ее осуществлять.

*Правила важны для:*

- обеспечения качественного управления;
- выбора номенклатуры выпускаемой продукции и общего процесса развития;
- демонстрации поддержки руководства;
- устранения препятствий;
- обеспечения последовательной и полной защиты вместо разрозненных усилий.

*Правила должны быть разработаны:*

- до возникновения проблем с безопасностью;
- для устранения препятствий в бизнесе;
- после прорыва защиты;
- для документального подтверждения соответствия стандартам качества и управления качеством (например, ISO 9001).

*Правила должны быть разработаны путем:*

- определения объема и целей разработки руководящих документов;
- определения того, какие правила должны быть разработаны;

- оценки степени риска или EDP (electronicdataprocessing — электронная обработка данных) аудита;
- выполнения тщательного обследования объекта, утверждения и претворения в жизнь инструкций.

### Обязанности в области информационной безопасности

*Обязанности руководства.* Обязанность руководства заключается не только в материально-технической и организационной поддержке. Недостаточно одного утверждения программы информационной безопасности. Руководство должно признать программу частью производственного процесса. Признание руководством программы информационной безопасности частью производственного процесса показывает, что отношение руководства к ней точно такое же, как и к другим задачам, стоящим перед организацией [2].

Обычно представители руководства не обучались технологии или основам информационной безопасности, они и не должны понимать, как это работает, но им необходимо быть уверенными, что их бизнес надежно защищен, а решения безопасности не мешают бизнес-процессу. Руководство намечает определенные цели для организации, а большинство профессионалов в сфере безопасности и информационных систем не вникают в эти нюансы.

Обе группы должны понимать, что безопасность является целью, за осуществление которой должны бороться обе эти стороны. Это становится ясно после анализа степени риска, стоимости и требований гарантии защищенности доступа к информации. Руководящий состав должен нести ответственность за проведение анализа и возложение обязанностей на технический персонал, отвечающий за внедрение правил информационной безопасности.

*Комитет по управлению информационной безопасностью.* Один из способов осуществить связь между двумя группами заключается в создании комитета по управлению информационной безопасностью (постоянно действующего совета, координационной группы и т. п.). В обязанности такого комитета будет входить контроль за изменениями в планировании бизнеса и определении того, каким образом правила информационной безопасности должны отражать эти изменения. Другой целью этого комитета может быть анализ производственных процессов и обеспечение гарантий соответствия их правилам безопасности, а также удовлетворение запросов на исключения из этих правил [3].

Для успешной работы комитета необходимо, чтобы в него входили специалисты различного профиля, наподобие состава группы, которая разрабатывает документы, определяющие политику безопасности. Однако этот комитет должен состоять из представителей руководства, которые будут понимать суть политики безопасности с экономических позиций и технических перспектив. Техническое руководство должно осознавать суть проблем бизнеса и иметь доступ к информации для того, чтобы оказывать помощь в принятии правильных решений по вопросам безопасности. Желательно, чтобы в комитете были представители и исполнительного персонала [2].

*Право на информацию.* Одной из самых сложных задач руководства или комитета по управлению является распределение ответственности за информационные ресурсы или средства управления ими, что также называется правом на информацию. Лицо, которому предоставлено право на информацию, становится ответственным за сохранность информационных активов согласно установленным правилам [10].

Для многих людей право на информацию представляет собой довольно непростую концепцию. В традиционной модели безопасности данные и средства управления ими хранятся на серверах под надзором администратора или администраторов. Администратор должен понимать, как функционирует система и как установить средства управления доступом. Проблемы начинаются тогда, когда администратор вынужден иметь дело с набором разнотипных средств управления большим числом разнотипных серверов, баз данных, средств хранения данных, т. е. ресурсов. Чтобы поддерживать ощущение порядка, администратор следует правилам, пытаясь привести их к единому знаменателю, как-то удовлетворяющему каждой из обслуживаемых им систем.

В этом сценарии администратор устанавливает классификацию, степень важности и средства управления доступом к информации согласно своим представлениям о работе. Нет гарантий того, что эти атрибуты будут соответствовать правилам безопасности в отношении каждого, кто имеет доступ к информации. Могут возникнуть конфликты между пользователями, требующими доступ к информации, и администраторами, которые приняли ошибочные решения.

В качестве альтернативного метода можно предоставлять право на данные и на средства управления. Ответственный за информацию будет отвечать за предоставление доступа к данным и определять, каким образом будет осуществляться управление данными. Для управления информационными активами ответственный за информа-

цию будет работать с администраторами безопасности и/или системными администраторами. Он сам будет определять степень важности и классифицировать информацию вместо того, чтобы оставлять это на попечение администратора. В результате управление информационными активами будет соответствовать нуждам ответственного за информацию лица.

Ответственное за информацию лицо будет отвечать за отклонения от общепринятой практики обработки информации. Если запрос на получение информации требует действий, нарушающих существующие правила, то ответственный за информацию будет отвечать за принятые отклонения от правил и за возможные последствия. В некоторых организациях от ответственного за информацию требуют письменного запроса на отклонения от правил, а также он должен подписать заявление о полной ответственности в случае возникновения потенциальных проблем. Поскольку никто не хочет излишне рисковать карьерой из-за такой ответственности, запросы на отклонения от правил появляются нечасто [5].

Обратная сторона права на информацию заключается в том, что ответственный за информацию должен обеспечивать доступ к информации в соответствии с требованиями правил безопасности. Некоторые ответственные за информацию считают несправедливым требовать от них полной ответственности и заставлять рисковать своей карьерой, поэтому они нарушают инструкции и игнорируют правила. Единственный способ решить эту проблему заключается в надлежащем обучении вопросам безопасности, в поддержке руководства и последовательном строгом контроле за соблюдением требований.

Другая проблема, связанная с правом на информацию, заключается в том, что эта схема хорошо работает только в таких организациях, где данные можно распределить среди потенциальных ответственных за информацию. Не замечено, чтобы такая схема хорошо работала в маркетинговых организациях или в таких компаниях, где данные полностью интегрированы в среде. Право на информацию также может стать проблемой в небольших организациях, в которых недостаточно людей для поддержания этой концепции. Одна из компаний, например, сделала каждого из 20 служащих совладельцами данных. Такая мера также помогала поддерживать целостность данных.

Если организацию не удовлетворяет предложенная концепция права на информацию, можно откорректировать правила так, чтобы они предусматривали создание ответственных комитетов. Такие небольшие комитеты выполняют ту же работу, что и ответственные за информацию, но ответственность несет не одно лицо, а группа лиц. Еще лучше, когда весь комитет является ответственной стороной. В этом случае при появлении запросов на отклонение от правил создается ситуация, требующая дополнительных проверок и согласований [3].

*Распределение прав на информацию.* Первое правило при распределении прав на информацию заключается в том, чтобы заинтересовать ответственного за информацию, сделав его собственником этих данных. Другими словами, ответственным за финансовую информацию должен быть кто-то, кто подчинен финансовому директору. Не стоит создавать массу различных подразделений, если это не согласуется с бизнес-процессом [2].

Это также означает, что отдел информатизации не должен являться ответственным за всю информацию, если только это необходимо для таких операций, как конфигурирование системы, идентификация пользователей, службы именования доменов и т. п. [3].

Обсудив право на информацию с теми, кто имеет к ней непосредственное отношение, можно выяснить их соображения по этому поводу. Они могут даже предложить варианты распределения или систематизации ответственности за информацию.

Права на информацию должны быть распределены на основе систематизации информационных активов верхнего уровня. Можно использовать те же результаты систематизации информации, которая была проведена во время подготовительных работ (описанных в первой части). Авторы рекомендуют использовать систематизацию верхнего уровня, так как в этом случае не будет слишком много лиц, ответственных за информацию. Это может потребовать дополнительного анализа того, кто и за какую информацию должен отвечать, но ограничение числа ответственных лиц даст возможность управлять этим процессом. Таким образом, в соответствии с классификатором информации каждый важный вид информации должен иметь назначенного ответственного за этот вид информации [2].

*Обязанности ответственных лиц за информацию.* Если организация приняла решение распределить права на информацию, необходимо рассмотреть, какие обязанности имеют ответственные за информацию лица. Инструкции, изложенные в правилах безопасности, должны определять круг лиц, ответственных за информацию и кому разрешен доступ к особым средствам управления информацией. Слово "особые" подразумевает, что ответственные за информацию имеют доступ

к таким средствам управления, с которыми не могут работать все остальные. Подобные формулировки правил могут быть составлены и для администрирования средств управления доступом в рамках тех функций, которые дозволены администратору [3].

Самая важная обязанность ответственного за информацию заключается в разрешении и отмене права доступа к информации компании. При разработке правил, которые связаны с правом доступа к информации, необходимо учитывать, что в правилах должна быть регламентирована работа и самого ответственного за информацию. Кроме того, в правилах доступа к информации необходимо оговорить возможность восстановления данных и функций управления доступом. В правилах могут быть следующие формулировки [2]:

- Если ответственное за информацию лицо будет отсутствовать, то необходимо назначить кого-то, кто будет действовать от его имени.
- Пароли, используемые при управлении информацией, должны содержать пароль или ключ, с помощью которого можно получить доступ к этим паролям в случае, если с ответственным за информацию что-то случится.
- Должны существовать механизмы для замены ответственного за информацию лица.

Следует помнить, что рассматриваемые механизмы являются частью правил безопасности.

*Согласование планов информационной безопасности.* При обсуждении обязанностей и служебного соответствия руководителей необходимо уделить внимание тому, как руководство следит за соблюдением правил, а также как оно реагирует на нарушения правил. Эти условия касаются не только поддержки руководства [6].

Необходимо обсудить роли, которые будет выполнять руководство в поддержку информационной безопасности.

При проведении обучения присутствие представителей руководства может быть эпизодическим и нерегулярным по сравнению с присутствием прочего персонала компании. Но не стоит разделять руководителей на какие-то категории. Лучше объединить их в едином плане безопасности, сделать руководство активным участником. Если нет необходимости контролировать системные журналы или проводить независимые проверки (хотя это может быть целесообразным), руководство может быть привлечено к организации совещаний, а также к рассмотрению дел служащих, которые нарушили правила безопасности. Если же проблемы затрагивают правовые аспекты, члены руководящего состава должны стать активными участниками расследования.

В процессе автоматизации бизнес-процессов руководство, которое не понимает технологии, старается спрятаться за спины технического персонала или консультантов. Несмотря на то что информационная безопасность не является техническим вопросом, все выглядит именно так. Один из способов включить руководство в процесс разработки политики безопасности заключается в том, чтобы сделать его ответственным за эти процессы подобно наделению правом на информацию управляющих нижнего уровня [6].

*Роль отдела информационной безопасности.* Отдел информационной безопасности отвечает за внедрение и сопровождение всего спектра документов, составляющих правила информационной безопасности организации, стандартов, инструкций и руководств. Этот отдел проводит обучение персонала основам безопасности и контролирует, чтобы каждый сотрудник знал свою роль в проведении политики безопасности, иначе отдел информационной безопасности обеспечивает механизмы, поддерживающие программу безопасности, намеченную политикой.

Этот отдел должен поддерживать баланс между образованием и административным принуждением В правилах безопасности для этого отдела должны быть четко определены все обязанности. Отдел должен рассматриваться как партнер в бизнесе, не вызывать негативную реакцию, что препятствует внедрению правил информационной безопасности [7].

*Интеграция информационной безопасности в бизнес-процесс организации.* Основной целью распределения обязанностей по защите информации является интеграция информационной безопасности в среду бизнеса. Один из этапов этой интеграции — определение должностей, которые обеспечивают безопасность всей работы. Например, один из способов осуществления этого заключается в распределении обязанностей и контроля над активами организации путем координирования работы каждого, включая ответственных за информацию и материально ответственных сотрудников. При таком подходе не возникнет непонимания относительно того, кто, за что и когда отвечает [2].

Еще одним аспектом исследований является вопрос организации управления безопасностью в организации. В организации формируется главная группа управления информационной безопасностью, она отвечает за внедрение и контролирует исполнение правил безопасности и процедур. Рассмотрим подход, принятый для неограниченных систем, когда главная группа управления информационной безопасностью назначает администраторов безопасности для многопользовательских

систем, в которых имеется большое число подразделений. В таком случае в каждом подразделении будет свой собственный сотрудник безопасности или посредник, который будет помогать внедрению программы безопасности подразделения. Подобным образом можно обеспечить более тесное сотрудничество тех, кто следит за безопасностью, с пользователями.

Тесный контакт сотрудников службы безопасности с остальным персоналом будет полезным и при управлении связями со сторонними организациями. Угроза безопасности исходит не только от собственных служащих, но и от клиентов, поставщиков, а также от каждого, кто, подключаясь к информационным активам организации, имеет возможность нарушить правила безопасности. Посредники должны отвечать за обучение перечисленных аутсайдеров, а также контролировать их деятельность и стимулировать ее. Так работают в небольших организациях. Во многих из них, особенно в сторонних организациях, немногочисленный персонал делят на "отделы", в которых одного человека назначают посредником со службой безопасности [2].

Однако это не лучшее решение. Некоторые сотрудники, работающие в организации достаточно большой период времени, могут найти способы разобраться в тонкостях работы системы и злоупотребить этим в своих целях. Единственный способ предотвратить злоупотребление — это не допускать пребывания сотрудника продолжительное время в роли посредника по безопасности (например, не более одного-двух лет). По истечении этого срока они передают свою работу другому. Другой способ заключается в том, чтобы установить порядок проверок и учета.

Система снабжения организации является одним из управляемых процессов. Даже несмотря на то, что большая часть закупок проходит этап утверждения руководством, часто такое утверждение проходит формально и оплата осуществляется без последующих уведомлений. Посредник безопасности в бухгалтерии будет следить за нарушениями в порядке закупок и отгрузки заказов [1].

Ревизор должен знать все тонкости бизнеса, особенности клиентов и поставщиков, знать старые и новые правила делопроизводства, а также — денежные потоки организации. Только тогда он сможет разобраться в счетах-фактурах и заявках на закупки и определить, нет ли в них нарушений [2].

Последним аспектом, который следует учесть в процессе реализации программы защиты информации, является цикл развития программного обеспечения. Независимо от того, разрабатывалось ли программное обеспечение собственными силами или организацией-подрядчиком, или были закуплены коммерческие программные продукты (COTS — CommercialOff-The-Shelf), целью должно быть создание безопасных систем, в которых можно легко локализовать ошибки или попытки вторжения. Внедрение стандартов кодирования и тестирования также будет содействовать обеспечению качественных производственных процессов. Более того, использование такой парадигмы, как живучесть, также может стать основой для проектирования программного обеспечения, с которым не будет проблем при развертывании или в процессе эксплуатации [8].

*Конкретные задачи информационной безопасности.* Единственным способом, гарантирующим, что любой из работающих в организации или принимаемый на работу служащий, или пользователь будет знать, что обеспечение безопасности является частью его работы, является внесение соответствующих записей в должностные инструкции. Изложение функциональных обязанностей и требований безопасности в должностных инструкциях демонстрирует сотруднику важность информационной безопасности и заставляет осознать, что она является неотъемлемой частью его работы. После того как эти обязанности и требования введены в должностные инструкции, к ним начинают относиться с пониманием того, что они влияют на оценку профессиональной пригодности работника [8].

Сторонние подрядчики, поставщики или другие лица, которые предоставляют услуги непосредственно в сети компании, должны включать подобные формулировки в свои рабочие предписания (SOW). Как и в случае с собственными служащими, такие записи документально подкрепляют обязательства компании, а также заставляют подрядчиков и поставщиков строго следовать требованиям безопасности организации, так как по этим показателям будет оцениваться качество предоставляемых ими услуг.

*Аудит и контроль.* Аудит и контроль важны при внедрении и контроле за соблюдением требований безопасности. Однако если эта работа не будет составной частью бизнес-процесса, есть вероятность, что эти меры никогда не будут осуществлены. Необходимо осознать, что эта работа является контролем качества выполнения программы информационной безопасности. В результате работа по обеспечению внутреннего аудита средств управления информационной системы будет выполняться постоянно, а не отдельными бросками.

Главное, на чем нужно сосредоточить внимание после совершения преступления, — это сбор улик. Поэтому в качестве этапа предварительной подготовки требуется ознакомиться с правилами сбора свидетельских показаний. Эти правила изложены в инструкциях, которыми руководствуются прокуроры или следственные работники при предоставлении показаний в суде или проведении следственных действий. Правила информационной безопасности нужно разрабатывать на основании этих инструкций, чтобы уметь правильно обработать данные, системы, сети и системные журналы после того, как было совершено преступление. Это нужно представить в виде четких руководств, прилагаемых к правилам, работая по которым можно быть уверенным в надлежащей защите улик. Нельзя забывать, что без предоставления соответствующих доказательств прокурор может использовать формулировку "за недостатком улик", и преступники окажутся на свободе [9].

*Обучение и поддержка в области защиты информации.* После разработки правил безопасности необходимо организовать обмен мнениями между разработчиками, руководством и каждым сотрудником организации, чтобы всем разъяснить предписания политики и ее значение. На этом заключительном этапе планирования необходимо запроектировать обучение персонала. Это обучение необходимо каждому, имеющему доступ к компьютерам и сетям компании. Сотрудники должны располагать необходимыми записями, включая программу обучения и сам курс обучения, а также все утвержденные документы принятых корпоративных правил безопасности.

Руководство должно не только выделить время на обучение, но и всячески поощрять его проведение. Предписания политики позволяют на некоторых предприятиях не выплачивать служащим жалованье (или платить по минимуму) до тех пор, пока они не пройдут курс обучения или не просмотрят его на видеопленке. Такой способ дает надежные результаты.

Следует помнить, что разработав большое число различных правил безопасности, нужно позаботиться, чтобы все они были применимы в конкретных условиях. Это означает, что невозможно спланировать программу обучения персонала одну для всех. Планы обучения должны быть тесно согласованы с политикой безопасности организации. Необходимо также понимать, что не каждому служащему требуется обучение по всем аспектам безопасности. При разработке планов и программ изучения правил безопасности следует помнить, что каждый аспект правил безопасности должен быть изучен соответствующим персоналом [3].

## Общие выводы

Для успеха программы защиты информации поддержка руководства имеет решающее значение. Наряду с заявленной поддержкой должна быть и ответственность за успешное претворение в жизнь этой программы. Особое значение авторы придают назначению ответственных руководителей и роли того персонала, который реализует административные меры внедрения правил безопасности. Программа безопасности будет иметь успех, если персонал и руководители будут хорошо знать свои функции и будут готовыми к решительным действиям. Этого можно добиться только в том случае, если каждый будет хорошо знать правила безопасности, пройдя полный курс по программе изучения информационной безопасности.

*Обязанности руководства:*

- участие и поддержка комитета по управлению информационной безопасностью;
- право на информацию включает распределение обязанностей по управлению информационными активами; назначаются ответственные за информацию, которые классифицируют информацию по степени ее важности и допускают отклонения в ее обработке от общепринятой практики;
- разработка и согласование с руководством планов защиты информации.

*Роль отдела информационной безопасности:*

- правилами должно быть установлено, что отдел информационной безопасности полностью отвечает за внедрение и сопровождение в организации правил информационной безопасности, стандартов, инструкций и процедур;
- отвечает за обучение, использование административных мер и покровительство со стороны руководства;
- при привлечении сторонних организаций или консультантов по информационной безопасности обеспечивает их работу по инструкциям, принятым для работы собственным отделом информационной безопасности.

*Прочие аспекты защиты информации:*

- необходимо распределить обязанности и ответственность за управление активами компании, координировать деятельность каждого, включая ответственных за информацию и материально-ответственных лиц;
- назначить администратора безопасности для всех многопользовательских систем, в каждом

подразделении выделить посредника по информационной безопасности;

- определить ответственных за безопасность обмена информацией со сторонними организациями в реальном времени;
- принять меры для судебного пересмотра платежей по закупкам и продажам, проведенным с нарушениями закона;
- включить положения об ответственности за соблюдение норм безопасности в должностные инструкции и в договора со сторонними организациями и следить за их соблюдением;
- ключевую роль занимает включенный в бизнес-процесс внутренний аудит средств управления информационными системами.

*Право на информацию и ответственность за ее сохранность:*

- при распределении прав на информацию отдел информационных систем не назначается ответственным за информацию, исключение составляет информация, с которой он непосредственно работает. Распределение прав на информацию должно быть проведено только после инвентаризации верхнего уровня информационных активов. Должен быть назначен по крайней мере один ответственный за каждый из основных типов информации;
- к распределению обязанностей по обеспечению безопасности информационных активов относится определение дозволенных средств управления и методов администрирования этих средств. Необходимо иметь инструкции для предоставления и лишения прав доступа к информационным активам компании, а также для восстановления информации в случае ее потери.

*Понятия управления безопасностью и применения закона:*

- знать и сознательно соблюдать законы и правила в пределах своих юридических прав;
- соблюдать правила сбора улик и обеспечивать юридические гарантии принятия их судом;
- предварительно планировать взаимодействие компании с органами правосудия и прокуратурой, чтобы на этой основе обрабатывать данные и проводить расследование в случае совершения преступления.

*Обучение и поддержка информационной безопасности:*

- обучаться должны все работники, имеющие доступ к компьютерам и сетям компании. Служащие должны подписать обязательства с требованиями пройти обучение, а также иметь на руках документ, подтверждающий прохождение курса обучения;
- руководство должно выделить время на обучение и способствовать его проведению;
- обучение должно отвечать требованиям политики безопасности.

**Нормативная база анализа защищенности**

Наиболее значимые нормативные документы в области информационной безопасности, определяющие критерии оценки защищенности автоматизированных систем, и требования, предъявляемые к механизмам защиты:

- общие критерии оценки безопасности информационных технологий (ИТ) (The Common Criteria for Information Technology Security Evaluation/ISO 15408);
- практические правила управления информационной безопасностью (Code of practice for Information security management/ISO 17799).

Кроме того, в России первостепенное значение имеют руководящие документы (РД) ФСТЭК России. В других странах их место занимают соответствующие национальные стандарты.

Наиболее полно критерии для оценки механизмов безопасности программно-технического уровня представлены в международном стандарте *ISO 15408: Common Criteriafor Information Technology Security Evaluation* (общие критерии оценки безопасности ИТ), принятом в 1999 г. [10].

Общие критерии оценки безопасности ИТ (далее "Общие критерии") определяют функциональные требования безопасности (security functional requirements) и требования к адекватности реализации функций безопасности (securityas surance requirements).

При проведении работ по анализу защищенности АС, а также средств вычислительной техники (СВТ) "Общие критерии" целесообразно использовать в качестве основных критериев, позволяющих оценить уровень защищенности АС (СВТ) с точки зрения полноты реализованных в ней функций безопасности и надежности реализации этих функций.

Хотя применимость "Общих критериев" ограничивается механизмами безопасности программно-технического уровня, в них содержится определенный набор требований к механизмам безопасности организационного уровня и требований по физической защите, которые непосредственно связаны с описываемыми функциями безопасности.

Первая часть "Общих критериев" содержит определение общих понятий, концепции, описание модели и методики проведения оценки безопасно-

сти ИТ; вводится понятийный аппарат и определяются принципы формализации предметной области.

Требования к функциональности средств защиты приводятся во второй части "Общих критериев" и могут быть непосредственно использованы при анализе защищенности для оценки полноты реализованных в АС (СВТ) функций безопасности.

Третья часть "Общих критериев" содержит класс требований по анализу уязвимостей средств и механизмов защиты под названием AVA (Vulnerability Assessment). Данный класс требований определяет методы, которые должны быть использованы для предупреждения, выявления и ликвидации следующих типов уязвимостей:

- наличие побочных каналов утечки информации;
- ошибки в конфигурации либо неправильное использование системы, приводящее к переходу системы в небезопасное состояние;
- недостаточная надежность (стойкость) механизмов безопасности, реализующих соответствующие функции безопасности;
- наличие уязвимостей ("дыр") в средствах защиты информации, позволяющих пользователям получать несанкционированный доступ НСД к информации в обход существующих механизмов защиты.

Соответствующие требования гарантированности оценки содержатся в следующих четырех семействах требований:

- AVA_CCA: Covert Channel Analysis (анализ каналов утечки информации);
- AVA_MSU: Misuse (ошибки в конфигурации либо неправильное использование системы, приводящее к переходу системы в небезопасное состояние);
- AVA_SOF: Strengthof TOE Security Functions (стойкость функций безопасности, обеспечиваемая их реализацией);
- AVA_VLA: Vulnerability Analysis (анализ уязвимостей).

При проведении работ по аудиту безопасности перечисленные семейства требований могут использоваться в качестве руководства и критериев для анализа уязвимостей АС (СВТ).

Наиболее полно критерии для оценки механизмов безопасности организационного уровня представлены в международном стандарте *ISO 17799: Code of Practice for Information Security Management* (практические правила управления информационной безопасностью), принятом в 2000 г. ISO 17799 является международной версией британского стандарта BS 7799 [11].

ISO 17799 содержит практические правила по управлению информационной безопасностью и может быть использовано в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты.

Практические правила разбиты на 10 разделов.

- Политика безопасности;
- Организация защиты;
- Классификация ресурсов и их контроль;
- Безопасность персонала;
- Физическая безопасность;
- Администрирование компьютерных систем и вычислительных сетей;
- Управление доступом;
- Разработка и сопровождение информационных систем;
- Планирование бесперебойной работы организации;
- Контроль выполнения требований политики безопасности.

В этих разделах содержится описание механизмов безопасности организационного уровня, реализуемых в правительственных и коммерческих организациях во многих странах мира.

Десять средств контроля, предлагаемых в ISO 17799 (они обозначены как ключевые), считаются особенно важными. Под средствами контроля в данном контексте понимаются механизмы управления информационной безопасностью организации.

При использовании некоторых из средств контроля, например шифрования данных, могут потребоваться советы специалистов по безопасности и оценка рисков, чтобы определить, нужны ли они и каким образом их следует реализовывать. Для обеспечения более высокого уровня защиты особенно ценных ресурсов или оказания противодействия особенно серьезным угрозам безопасности в ряде случаев могут потребоваться более сильные средства контроля, которые выходят за рамки ISO 17799.

Десять ключевых средств контроля, перечисленных далее, представляют собой либо обязательные требования, например требования действующего законодательства, либо считаются основными структурными элементами информационной безопасности, например, обучение правилам безопасности. Эти средства контроля актуальны для всех организаций и сред функционирования АС и составляют основу системы управления информационной безопасностью. Они служат основой для организаций, приступающих к реализации средств управления информационной безопасностью.

Ключевыми являются следующие средства контроля:

- документ о политике информационной безопасности;
- распределение обязанностей по обеспечению информационной безопасности;
- обучение и подготовка персонала к поддержанию режима информационной безопасности;
- уведомление о случаях нарушения защиты;
- средства защиты от вирусов;
- планирование бесперебойной работы организации;
- контроль над копированием программного обеспечения, защищенного законом об авторском праве;
- защита документации организации;
- защита данных;
- контроль соответствия политике безопасности.

Процедура аудита безопасности АС включает в себя проверку наличия перечисленных ключевых средств контроля, оценку полноты и правильности их реализации, а также анализ их адекватности рискам, существующим в данной среде функционирования. Составной частью работ по аудиту безопасности АС также являются анализ и управление рисками.

**Литература**


1. *Бармен С.* Разработка правил информационной безопасности / Пер. с англ. — М.: Издательский дом Вильяме, 2002. — 208 с.

2. Иллюстрированный самоучитель по разработке безопасности. [Электронный ресурс]. Режим доступа: http://samoychiteli.ru/document34390.html

3. Прога онлайн — сервисы и мобильные приложения [Электронный ресурс]. Режим доступа: https://progaonline.com/

4. *Титов А. А.* Двадцать основных принципов, без которых нельзя обойтись при создании надежного программного обеспечения [Электронный ресурс]. Режим доступа: https://www.rsdn.org/article/20princ/20principles.xml

5. *Нестеров В.* Международные стандарты качества ISO 9000 [Электронный ресурс]. Режим доступа: https://www.quality.eup.ru/GOST/ms_iso9000.htm

6. Иллюстрированный самоучитель по Developmentofsafety [Электронный ресурс]. Режим доступа: http://www.access-vba.forekc.ru/015/index.htm

7. Разработка автоматизированной информационной системы учета проведения инструктажей по вопросам информационной безопасности [Электронный ресурс]. Режим доступа: https://vuzlit.ru/986050/razrabotka_avtomatizirovannoy_informatsionnoy_sistemy_ucheta_provedeniya_instruktazhey_po_voprosam_informatsionnoy_bezopasnosti

8. Должностная инструкция ревизора, должностные обязанности ревизора, образец должностной инструкции ревизора [Электронный ресурс]. Режим доступа: https://www.rabota.ru/articles/hr/dolzhnostnaja_instruktsija_revizora_dolzhnostnye_objazannosti_revizora_obrazets_dolzhnostnoj_instruktsii_revizora_3912

9. Организация и проведение внутреннего аудита информационной безопасности [Электронный ресурс]. Режим доступа: https://otherreferats.allbest.ru/audit/00342487_0.html

10. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/1200101777

11. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-17799-2005


# Ways to involve the management team in the development of corporate network security policies


*A. S. Vilkov, M. M. Taraskin*
Military unit № 11928, Moscow, Russia



*The article deals with ways to involve the management of organizations in activities to create its comprehensive security. One of the important directions in this process is to develop a security policy for corporate networks. We consider a set of step-by-step measures aimed at forming a security policy in the organization, in particular, corporate networks. The materials are considered with varying degrees of detail activities in the areas of regulatory, organizational, as well as hardware and software. The conclusions provide specific recommendations for overcoming the "passive" attitude of the organization's management staff to measures to create its comprehensive security, as well as the guiding documents (RD) of the FSTEC of Russia related to the problem under consideration.*



*Keywords:* security policy of corporate networks, information security, threats, vulnerabilities and risks, information, information protection.

Bibliography — 11 references. *Received January 26, 2020*

УДК 004.056.53

# Автоматизированная система мониторинга окружающей среды как объект защиты информации

*А. В. Шарамок*, канд. техн. наук
Национальный исследовательский университет "МИЭТ", г. Зеленоград, Москва, Россия

*Проведен анализ требований по защите экологической информации, на основе которого сформулированы высокоуровневые требования по обеспечению безопасности информации в автоматизированной системе мониторинга окружающей среды (АСМОС). На основании высокоуровневых требований рассмотрены два аспекта обеспечения доверия при использовании АСМОС: уверенность в соответствии целям безопасности и достоверность предоставляемой информации. Сформулированы предположения безопасности и предположения о защищаемых активах АСМОС.*

*Ключевые слова*: экологическая и метеорологическая информация, подлинность информации, доверие, среда безопасности.

Активная деятельность человечества меняет окружающую среду. Эти изменения приобретают все более негативный характер. Измерение, хранение и обработка информации об окружающей среде становятся важными как для обеспечения сохранности исторических значений, так и для обеспечения безопасности жизнедеятельности населения. Отсутствие своевременной и объективной информации о состоянии параметров окружающей среды (уровень радиации, наличие загрязнений и т. д.) может спровоцировать панику среди населения и стать причиной социальных волнений. Примером подобной ситуации может служить инцидент на полигоне в Архангельской области 8 августа 2019 г. [1], когда задержка в информировании населения и его потенциальное недоверие к официальной информации могли спровоцировать панику [1]. При этом информация из официальных источников [2] не вызывала должного доверия со стороны населения, так как традиционные технологии сбора, обработки и предоставления экологической информации оставляют потенциальную возможность для манипуляций.

Применение АСМОС позволяет, во-первых, существенно сократить время доведения актуальной информации до заинтересованных потребителей (обеспечить своевременность), во-вторых, используя технические решения, обеспечить ее достоверность, минимизируя возможности субъективного вмешательства. Обеспечение актуальности и достоверности информации в автоматизированных системах относится к вопросам защиты информации (информационной безопасности) [3]. Именно с этой точки зрения автор предлагает рассмотреть АСМОС. Необходимо отметить, что даже актуальная и достоверная информация, предоставляемая автоматизированной системой, оставляет возможность манипулирования общественным сознанием [4]. Этот вопрос выходит за рамки технических проблем и в данной работе рассматривать не будем.

**Шарамок Александр Владимирович**, доцент кафедры ТКС.
E-mail: aleksandr.sharamok@org.miet.ru

*Статья поступила в редакцию 5 февраля 2020 г.*



## Состав АСМОС

Система АСМОС предназначена для сбора, обработки, хранения и передачи метеорологических величин (температура *T*, относительная влажность RH, давление *P*, скорость и направление ветра *V* и *Vn*) и экологических величин (основные загрязнители воздуха – PM, CO, NO, $NO_2$, $SO_2$ и $O_3$, свет, шум и некоторые виды ионизирующих излучений) [5, 6].

Для рассматриваемой в [5, 6] модели АСМОС необходимо выделить следующие основные компоненты:

- измерительные посты (мобильные и стационарные) с совокупностью входящего в их состав аппаратно-программного обеспечения как средства первичного сбора, накопления и обработки информации;
- инфраструктура LoRaWAN как механизм взаимодействия между измерительными постами и серверным приложением;
- серверное приложение как средство обработки, хранения и предоставления данных, реализованное на облачной платформе;
- автоматизированные рабочие места как средства доступа конечных пользователей к информации.

Требования по защите информации целесообразно предъявлять к такой группировке компонент АСМОС, на данном этапе излишне не вдаваясь во внутреннюю структуру указанных групп.

## Анализ нормативных требований по защите информации в АСМОС

АСМОС осуществляет сбор, передачу, хранение и обработку экологической и метеорологической информации. В связи с этим требования по информационной безопасности (защите информации) к АСМОС будут предъявляться в соответствии с существующей нормативно-правовой базой по обработке, хранению и защите экологической информации и требованиями к автоматизированным системам. Учитывая это, необходимо сформировать перечень первичных документов, являющихся основой для формирования требований к АСМОС. Принципиально эти документы можно разделить на два вида: 1 — Конституция, законы и подзаконные акты, международные обязательства Российской Федерации; 2 — технические регламенты и требования, стандарты и требования регуляторов.

Анализ существующих правовых документов и международных обязательств Российской Федерации с точки зрения высокоуровневых требований по защите экологической информации проведен в [7]. В [7] указано на наличие противоречий в законодательстве и предлагается установить режим открытого доступа к экологической информации. На основании анализа указанных в [7] документов можно заключить, что засекречивание экологической информации и иное ограничение доступа к ней являются незаконными. Следующий важный вывод из [7]: из свойств защищенности информации на примере гексады Паркера [3] для АСМОС актуальными являются требования по обеспечению целостности, доступности, подлинности и владению. Требования по обеспечению конфиденциальности и полезности с точки зрения защиты информации к АСМОС не предъявляются: конфиденциальность — по причине отсутствия подобного требования со стороны нормативных документов и полезность — по причине обеспечения этого требования в рамках целевого использования АСМОС.

Из существующих технических регламентов, требований, стандартов и требований регуляторов с точки зрения защиты информации в отношении АСМОС необходимо выделить комплекс стандартов на автоматизированные системы и ГОСТ Р 51624-2014 [8], уточняющий эти документы в части автоматизированных систем в защищенном исполнении. При формировании требований по защите информации в АСМОС предлагается руководствоваться стандартами ГОСТ Р ИСО/МЭК 15408 [9], которые отражают передовую методологию по разработке защищенных продуктов информационной технологии (ИТ).

Анализ [7] не позволяет сделать вывод о наличии требований в нормативных документах по обязательной криптографической защите информации в АСМОС. В случае отсутствия подобных требований в дальнейшем при разработке АСМОС предлагается при формировании требований вместо документов, существующих в рамках Положения ПКЗ-2005 [10], руководствоваться международным стандартом ISO/IEC 19790:2012 [11].

Необходимо отметить, что в отношении АСМОС применимы и другие документы по защите информации (например, документы ФСТЭК России), но их целесообразно рассматривать на следующих этапах декомпозиции.

## Обеспечение доверия к системе АСМОС

Существует несколько определений технических терминов "доверие" и "доверенный продукт". Можно выделить два основных контекста использования термина "доверие" для АСМОС. Первый контекст подразумевает доверие пользователей к АСМОС как технической системе. Второй контекст подразумевает подтверждение подлинности получаемой от АСМОС информации.

Для первого контекста в ГОСТ Р ИСО/МЭК 15408 [9] дается следующее определение доверия: основа для уверенности в том, что продукт ИТ отвечает целям безопасности. Под соответствием целям безопасности понимается наличие некоторого желаемого функционала, соответствующего некоторым требованиям (спецификации) и отсутствие нежелательного функционала. Как правило, весь функционал, который не является желаемым, должен отсутствовать. При этом, как и в большинстве других нормативных документов, ГОСТ Р ИСО/МЭК 15408 [9] предполагает, что доверие обеспечивается с использованием активного исследования. Активное исследование — это оценка продукта ИТ для определения его свойств безопасности, что в отечественной практике принято называть сертификацией.

Следствием осознания того, что подобный подход недостаточен, является, например, создание "Единого реестра российских программ для электронных вычислительных машин и баз данных". Недостаточность обусловлена двумя обстоятельствами: во-первых — это возрастающая сложность ИТ-продуктов, что приводит к сопоставимости по

сложности задачи исследования ИТ-продукта с задачей разработки аналогичного ИТ-продукта; во-вторых — это ориентированность данного подхода на добросовестного разработчика. Недобросовестный разработчик, зная методы исследования ИТ-продуктов и пользуясь первым обстоятельством, может заложить нежелательный функционал, например закладки второго, третьего или последующих уровней в программном обеспечении. Оба этих фактора в конечном итоге приводят к невозможности выполнения задачи сертификации для гарантированного доверия к результатам исследования произвольного ИТ-продукта.

Исследователи данной проблемы (как отечественные, так и зарубежные), например С. П. Расторгуев [4], указывают, что единственной гарантией доверия к ИТ-продукту является доверие к разработчику ИТ-продукта. При этом доверие к разработчику можно разделить на две составляющие: обеспечение необходимой квалификации разработчика (может быть подтверждено методами активного исследования) и обеспечение лояльности разработчика (подтверждается нетехническими методами, например государственная принадлежность, обеспечением соответствующих допусков отдельных лиц и т. д.) и производителя ИТ-продукта (подтверждается наличием доверенного технологического маршрута изготовления ИТ-продукта).

На основании изложенного сформулируем следующие требования доверия к системе АСМОС:

- компоненты системы АСМОС на различных уровнях декомпозиции должны быть созданы доверенными разработчиками и производителями;
- компоненты АСМОС на ряде функциональных уровней декомпозиции должны быть созданы с учетом безопасного дизайна. В основе безопасного дизайна должны лежать обеспечение доверенных функций безопасности и использование доверенных криптографических методов;
- для обеспечения безопасного дизайна должны быть разработаны требования (спецификации) по безопасности к компонентам АСМОС на соответствующих функциональных уровнях декомпозиции. Требования должны разрабатываться в соответствии с методологией ГОСТ Р ИСО/МЭК 15408 [9]. Набор требований должен определяться по результатам декомпозиции системы АСМОС.

Указанные требования также отражают порядок достижения доверенности к произвольному ИТ-продукту. Не имеет смысла проводить активное исследование ИТ-продукта, если он не вышел от доверенного разработчика и производителя, т. е. на активное исследование доверенным разработчиком должен передаваться ИТ-продукт, в основе которого лежит безопасный дизайн. После подтверждения его соответствия требованиям по безопасности ИТ-продукт должен производиться и поставляться в соответствии с доверенным технологическим маршрутом.

### Обеспечение доверия (подлинности) данных АСМОС

В отношении контекста понятия доверия подлинности получаемой от АСМОС информации наиболее распространенным и технически удобно реализуемым является аутентификация взаимодействующих субъектов с использованием криптографических методов, например инфраструктуры открытых ключей. Инфраструктура открытых ключей является наиболее подходящим методом ключевого обеспечения для гражданских систем с большим числом участников взаимодействия. Как правило, инфраструктура открытых ключей подразумевает взаимодействие физических лиц с использованием вычислительных сетей. В связи с развитием таких направлений, как Интернет вещей, видимо, использование инфраструктуры открытых ключей будет смещаться в область межмашинного взаимодействия.

Как было отмечено, требуемыми характеристиками безопасности информации для системы АСМОС являются целостность, доступность, подлинность и владение.

Подлинность подразумевает, что информация на всех этапах ее жизненного цикла и с течением времени остается достоверной с некоторой допустимой погрешностью. Эта погрешность может возникнуть в процессе измерений или в процессе выполнения вычислительных процедур и носит предсказуемый характер, определяемый точностью измерительных и вычислительных средств.

Для защиты от намеренных и непреднамеренных искажений необходимо использовать специальные механизмы защиты. Эти механизмы принципиально можно разделить на два типа:

- зависящие от третьей доверенной стороны;
- независящие от третьей доверенной стороны.

Примером механизма, зависящего от третьей доверенной стороны, является упомянутая инфраструктура открытых ключей. При наличии достаточно очевидных положительных моментов от использования этой технологии существуют и явные недостатки. Например, безопасность инфраструктуры открытых ключей строится в предположении о доверии к удостоверяющему центру и другим элементам инфраструктуры открытых ключей. Появляется все больше фактов, подтвер-

ждающих, что подобное предположение является излишне оптимистичным [12]. Дополнительно у инфраструктуры открытых ключей имеются очевидные экономические трудности: высокая стоимость поддержания в актуальном состоянии ключевого материала, что особенно важно для таких технологий, как Интернет вещей.

Примером механизма без использования третьей доверенной стороны является технология блокчейн (распределенный реестр) [13]. Преимуществом этой технологии является то, что доверие к системе основано на экономически мотивированном корректном поведении участников. Отдельные отклонения поведения участников (даже достаточно большого числа) от логики разумного поведения не нарушают безопасность системы, а проведение успешных целенаправленных атак требует ресурсов (экономических, технических, человеческих и прочих), значительно превышающих эффект от реализации атак.

Применение в системе АСМОС технологии блокчейн позволит обеспечить подлинность метеорологических и экологических данных в процессе их хранения в системе. При этом возможна реализация двух вариантов: с обеспечением подлинности данных и с обеспечением контроля целостности данных. Первый вариант является более затратным по сравнению со вторым, но обладает очевидным преимуществом.

Суть решения заключается в записи в публичный блокчейн на каком-то из этапов обработки данных самих данных или их цифрового отпечатка (хеш-значения). Подобная запись приведет к сохранению (на время существования реестра) в блокчейне записанных данных или их отпечатка, что позволит в дальнейшем пользователям системы осуществлять контроль подлинности данных в системе АСМОС.

## Защищаемые информационные активы АСМОС

К защищаемым информационным активам АСМОС относятся целевая информация АСМОС (метеорологическая и экологическая), опасная информация криптографических средств и средств защиты от несанкционированного доступа, технические средства измерительных постов, программное обеспечение измерительных постов, серверных приложений и автоматизированных рабочих мест.

К опасной информации относится информация, раскрытие или модификация которой со стороны нарушителя (источника угроз) может привести к нарушению безопасности АСМОС.

В качестве защищаемых активов не рассматривают инфраструктуру Интернет, аппаратуру облачной среды и автоматизированных рабочих мест, часть программных средств облачной среды и автоматизированных рабочих мест, за которые ответственен провайдер облачных услуг. Как минимум из рассмотрения исключаются операционные системы облачной среды, программное обеспечение средств виртуализации и программное обеспечение промежуточного слоя (такое, как СУБД, программное обеспечение WEB-сервера). Состав исключаемого программного обеспечения облачной среды зависит от модели использования облачной среды. Ответственность за безопасность исключаемых компонент возлагается на провайдера облачных сервисов. Из защищаемых активов исключаются базовые станции и вся инфраструктура LoRaWAN. Предполагается, что вопросы безопасности при использовании инфраструктуры LoRaWAN [14] входят в ответственность соответствующих провайдеров. Из защищаемых активов также исключается операционная система АРМов по причине необходимости обеспечения мобильности пользователей системы. Предполагается, что используемые в составе АРМов операционные системы имеют и надлежащим образом используют как собственные, так и внешние средства обеспечения безопасности.

В целях удобства использования ссылок на защищаемые информационные активы введены их обозначения. Защищаемые информационные активы имеют обозначения следующего вида: А.<Название защищаемого информационного актива>. Названия защищаемых информационных активов выбраны с точки зрения краткости, удобства и уникальности названия.

К защищаемым информационным активам системы АСМОС относятся следующие.

- А.ИНФ_ОКРУЖ_СРЕДЫ

Информация метеорологических и экологических величин на всех этапах ее получения, передачи, хранения и обработки в АСМОС.

- А.ОИ

Опасная информация — секретные криптографические ключи симметричных и асимметричных криптографических алгоритмов, промежуточные гаммы криптографических вычислений, исходные случайные числа (ключ формирования случайных чисел, внутренние состояния датчиков случайных чисел) и промежуточные значения функции усложнения датчиков случайных чисел.

- А.СЕКРЕТ

Пароли пользователей вычислительных средств и другая аутентификационная информация, доступ к которой должен быть ограничен.

- А.ТЕХСРЕДСТВА

Технические средства измерительных постов в полном составе, к которым относятся аппаратные компоненты, реализующие целевую функцию АСМОС и защиту информации в измерительных постах.

- А.ПРОГРАММЫ

Программное обеспечение измерительных постов, серверных приложений и автоматизированных рабочих мест.

- А.АУДИТ

Записи аудита событий безопасности, ведущиеся в вычислительных средствах измерительных постов, серверных приложений и программном обеспечении автоматизированных рабочих мест.

### Предположения среды безопасности

Предположения безопасности описывают особенности безопасности среды, в которой предполагается эксплуатация АСМОС. Представленные предположения безопасности включают в себя:

1. Информацию об особенностях предполагаемого использования АСМОС, включая такие аспекты, как область применения АСМОС, ограничения применения АСМОС и т. п.;

2. Информацию об отдельных особенностях среды и условиях эксплуатации АСМОС, включая такие аспекты, как физическая защита, управление, сопровождение разработчиками и т. д.

Предположения безопасности имеют обозначения следующего вида: П.<Название предположения>. Названия предположений выбраны с точки зрения краткости, удобства и уникальности названия.

*Предположения о защищаемой информации*:

П.ИНФ_ИСТОЧНИКИ

Целевая информация, защищаемая в АСМОС, порождается в измерительных постах.

П.ИНФ_ПОТРЕБИТЕЛИ

Целевая информация, защищаемая в АСМОС, используется эксплуатационным персоналом АСМОС и неограниченным кругом сторонних пользователей.

П.ИНФ_ДОСТУП

Целевая информация, защищаемая в АСМОС, доступна пользователям в соответствии с их правами доступа. Часть целевой информации доступна неограниченному кругу пользователей.

П.ИНФ_СРЕДСТВА_ДОСТУПА

Доступ к целевой информации осуществляется через программное обеспечение АРМов и через WEB-интерфейс серверных приложений.

*Предположения физической безопасности*:

П.ФИЗ_ДОСТУП_ОБЛАКО

Вопросы защиты физического доступа к аппаратуре и программного обеспечения облачной среды и инфраструктуры LoRaWAN не входят в рамки задач АСМОС.

П.ФИЗ_ДОСТУП_ПОСТЫ

Физическая защита измерительных постов АСМОС осуществляется только в местах их хранения.

П. ФИЗ_ЦЕЛОСТНОСТЬ_ПОСТЫ

Контроль физической целостности аппаратуры измерительных постов осуществляется не реже, чем раз в 6 месяцев. При необходимости контроль физической целостности может осуществляться в течение не более одной недели после появления подозрений на нарушение целостности.

П.ФИЗ_ЗАХВАТ

Возможен только явный захват технических средств измерительных постов с оповещением ответственного эксплуатационного персонала после проведения контроля физической целостности.

П.ФИЗ_ЭКСТЕРРИТОРИАЛЬНОСТЬ

АСМОС эксплуатируется на территории Российской Федерации.

*Предположения об эксплуатационном персонале*:

П.ПЕРСОНАЛ_ОПЕРТИВНОЕ_УПРАВЛЕНИЕ

Оперативное управление осуществляется только эксплуатационным персоналом, имеющим подготовку и знания в объеме эксплуатационной документации. При осуществлении оперативного управления эксплуатационный персонал применяет только средства, предусмотренные эксплуатационной документацией, в случае возникновения ситуаций, для решения которых недостаточно средств, предусмотренных эксплуатационной документацией, эксплуатационный персонал обращается к разработчикам АСМОС.

П.ПЕРСОНАЛ_СОПРОВОЖДЕНИЕ

Система АСОМС находится на сопровождении разработчиков, т. е. устранение технических неполадок и разбор возникших сбоев и неисправностей осуществляется лицами, имеющими квалификацию и уровень знаний в объеме разработчика. Время реакции разработчиков на требования эксплуатирующей организации по проведению работ по сопровождению до одного месяца.

П.ПЕРСОНАЛ_СОСТАВ

Персонал АСМОС разделяется на эксплуатационный персонал (эксплуатирует измерительные посты, серверное программное обеспечение, дистрибутивы программного обеспечения АРМ), персонал безопасности и персонал технической поддержки.

П.ПЕРСОНАЛ_БЕЗОПАСНОСТИ

Для персонала безопасности определены следующие роли:

- администратор безопасности осуществляет все операции по настройке средств аутентификации и управлению доступом, работе с криптографическими средствами и ключевой информацией (генерация, хранение, распределение и т. д.), удаленному управлению и загрузке ключей;
- аудитор безопасности осуществляет доступ к журналам аудита криптографических средств и журналам аудита событий безопасности (настройка журнала, просмотр и удаление).

П.ПЕРСОНАЛ_ПОДДЕРЖКИ

Персонал технической поддержки осуществляет все операции по сборке, модификации, ремонту и настройкам аппаратного обеспечения, инсталляции и настройки общего и специального программного обеспечения.

*Предположения о внешних связях*:

П.ВНЕШНИЕ_СВЯЗИ

Все компоненты АСМОС подклеены к сети Интернет и используют ее для передачи информации.

*Прочие предположения*:

П.РЕЗЕРВИРОВАНИЕ

Резервирование работы компонент АСМОС, информационного содержимого и параметров конфигурации осуществляется ответственным эксплуатационным персоналом в соответствии с установленным регламентом и с использованием предусмотренных для этого в составе технических средств и организационно-технических мер.

П.СРЕДСТВА_РАЗРАБОТКИ

В составе программного обеспечения компонент АСМОС отсутствуют средства модификации объектного и программного кода, а также средства разработки и отладки программного обеспечения.

П.ВОЗМОЖНОСТЬ_ВОССТАНОВЛЕНИЯ

Восстановление работоспособности и ремонт технических средств измерительных постов осуществляются в условиях предприятия-изготовителя в срок до одного месяца.

П.ПОЛИТИКА_БЕЗОПАСНОСТИ

АСМОС управляется персоналом в пределах его полномочий в соответствии с положениями политики безопасности, изложенной в соответствующей документации.

## Заключение

Приведенный анализ позволил сформулировать высокоуровневые требования по обеспечению безопасности информации в АСМОС: доступность сервисов и достоверность (подлинность) собираемых, хранимых и обрабатываемых данных. С этой точки зрения при эксплуатации АСМОС должна обеспечиваться уверенность (доверие) в том, что АСМОС соответствует целям безопасности. Сформулированные предположения безопасности и предположения о защищаемых активах в совокупности с моделью источника угроз, изложенной в [15], позволят в дальнейшем разработать модель угроз для АСМОС и сформулировать ее цели безопасности, что в конечном итоге позволит разработать профиль безопасности или задание по безопасности в соответствии с методологией общих критериев безопасности информационных технологий [9].

**Литература**


1. Бизнес ФМ, "Была легкая паника". Какова обстановка в Северодвинске после взрыва на военном полигоне? [Электронный ресурс]. Режим доступа: https://www.bfm.ru/news/421491 (дата обращения: 17.01.2020).
2. Росгидромед, об аварийном, экстремально высоком и высоком загрязнении окружающей среды и выявленных случаях изменения радиационной обстановки на территории Российской Федерации в период с 5 по 16 августа 2019 года, подписано начальником УМСЗ Росгидромета Ю. В. Пешковым [Электронный ресурс]. Режим доступа: http://www.meteorf.ru/product/infomaterials/91/19651/ (дата обращения: 17.01.2020).
3. *Олифер В. Г., Олифер Н. А.* Безопасность компьютерных сетей. — М.: Горячая линия—телеком, 2019. — 644 с.
4. *Расторгуев С. П.* Информационная война. — М.: Радио и связь, 1999. — 416 с.
5. *Muratchaev S., Bakhtin A., Volkov A., Ivanov V., Baskakov A.* Modeling the Process of Network Scaling for LoRaWan Based on NS3: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), January 29 — February 01, 2018 Moscow and St. Petersburg, Russia, 2018. P. 1309—1312.
6. *Севрюкова Е. А., Волкова Е. А., Угроватов А. В., Копылова М. Д.* Имитационное моделирование системы мониторинга окружающей среды // Изв. вузов. Электроника. 2019. Т. 25. № 5. С. 521—529.
7. *Мисник Г. А.* Право на доступ к экологической информации // Журнал российского права. 2007. № 3. С. 83—92.
8. ГОСТ Р 51624-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.
9. ГОСТ Р ИСО/МЭК 15408-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
10. Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005). Утверждено Приказом ФСБ России № 66 от 9 февраля 2005 года.
11. ISO/IEC 19790:2012 Information technology — Security techniques — Security requirements for cryptographic modules.

12. *Рассохин А.* Электронная подпись оставила без квартиры [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/3969174 (дата обращения: 17.01.2020).

13. *Satoshi Nakamoto.* Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]. Режим доступа: https://nakamotoinstitute.org/bitcoin/ (дата обращения: 17.01.2020).

14. *Шарамок А. В.* Анализ безопасности стандарта связи LoRaWAN // Вопросы защиты информации. 2019. № 4 (127). С. 13—25.

15. *Шарамок А. В.* О методе разработки модели источника угроз // Вопросы защиты информации. 2013. № 1 (100). С. 26—31.

## The environment monitoring system as an information security asset

*A. V. Sharamok*
National Research University MIET, Zelenograd, Moscow, Russia

*There is a security requirements analysis for environmental and meteorological information provided in the article. According to the analysis high-level information security requirements are stated for the environment monitoring system (EMS). Based on high-level requirements, two aspects of ensuring trust for the EMS are considered: assurance to security goals and confidence to information. Security assumptions and assumptions about the EMS's assets are stated.*

*Keywords*: environmental and meteorological information, authenticity of information, trust, security environment.

Bibliography — 15 references. *Received February 5, 2020*

УДК 004

# Оптимизация времени доступа к динамической памяти при вычислении нейронных сетей на ПЛИС

[1, 2] *А. С. Кущенко*; [1] *О. Б. Макаревич*, д-р техн. наук; [1] *И. Ю. Половко*, канд. техн. наук
[1] Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, г. Таганрог, Ростовская обл., Россия
[2] АО «Научно-конструкторское бюро вычислительных систем», г. Таганрог, Ростовская обл., Россия

*Проведены исследования способов организации расчета отдельных слоев сверточных нейронных сетей и возможности оптимизации числа обращений к внешней памяти применительно к обработке изображений. Кратко описан самый распространенный порядок расчета результата слоем нейронной сети, а также описаны недостатки такого подхода. В качестве альтернативы предложены два метода, которые имеют преимущества на различных этапах обработки данных нейронной сетью. Полученный метод расчета слоя сверточной нейронной сети позволяет значительно сократить нагрузку на внешнюю память. Для оценки эффективности использованы теоретические расчеты по количеству данных, которые необходимо прочитать из внешней памяти. Оценка произведена для возможности работы ПЛИС с динамической памятью типа DDR3 или DDR4. Использование динамической памяти является более близким условием к реальным, чем любой иной тип ОЗУ, ввиду ее низкой стоимости и высокой емкости.*

*Ключевые слова*: сверточные нейронные сети, ПЛИС, обработка изображений, искусственный интеллект.

Все большее распространение получают сверточные нейронные сети (СНС). СНС имеют широкий круг применения: от распознавания образов на изображениях до принятия решения о направлении движения транспортных средств и поиска уязвимостей в текстах программного обеспечения [1].

СНС требуют большого количества памяти для хранения весов. Например, для нейросети YOLO [2] требуется примерно 200 Мбайт для хранения весов (веса в данном случае — ядра свертки и смещение для сверточных слоев и веса стимулов нейронов, порог активации и смещение для полносвязных слоев). Подобные объемы целесообразно хранить в динамической памяти (SDRAM или DDR), т. к. она намного дешевле статической (SRAM), имеет больший объем, чем накристальная память ПЛИС, и большую производительность, чем постоянные запоминающие устройства (ПЗУ). Все программные реализации (на CPU или GPU) и открытые аппаратные используют динамическую память для хранения весов. Однако у динамической памяти есть один недостаток: она показывает высокую производительность только при пакетных операциях чтения или записи, но при одиночных операциях максимальная скорость может составлять менее 10 % от теоретической. Из-за данной особенности динамической памяти разработчики нейронных сетей предлагают различные варианты упаковки весов, уменьшения разрядности весов и тому подобные методы уменьшения общего объема [3, 4]. Подобные меры необходимы из-за того, что программная реализация алгоритма СНС не управляет кешированием данных и при обработке постоянно читает данные из внешней памяти.

Вследствие большого количества весов для преобразования требуется большая пропускная способность внешней памяти для обеспечения достаточной скорости чтения и записи. Быстродействия одной микросхемы типа DDR4 с шиной данных 32 бита на частоте 2666 МГц [5] недостаточно для обеспечения своевременного чтения данных для обработки. Появляется необходимость оптимизации работы с внешней памятью.

Рассмотрена оптимизация работы с внешней памятью на примере СНС для распознавания изображений.

**Кущенко Андрей Сергеевич**, аспирант, конструктор 2-й категории.
E-mail: andrew.kushchenko@gmail.com
**Макаревич Олег Борисович**, профессор, заведующий кафедрой "Безопасность информационных технологий".
E-mail: mak@tsure.ru
**Половко Иван Юрьевич**, доцент.
E-mail: iypolovko@tsure.ru

*Статья поступила в редакцию 9 декабря 2019 г.*

### Метод организации порядка расчета слоя СНС

При обработке изображения СНС возможны два варианта расчета сверточного слоя, а именно вычисление:

- одной выходной карты признаков за проход (первый способ вычисления);
- всех выходных карт признаков одновременно (второй способ вычисления).

Проход — операция чтения изображения из памяти и применение к нему матрицы свертки.

Количество входных данных, которые необходимо прочитать для расчета выходного слоя первым способом, составляет

$$S_{p1} = whd_{\text{in}}d_{\text{out}}, \quad (1)$$

где $S_{p1}$ — суммарное количество пикселей для чтения;
$w$ — ширина изображения в словах (т. к. после первого слоя уже некорректно слово "данные", для обработки пикселями далее используем термин "слово", соответствующий разрядности данных, которая может в разных реализациях отличаться);
$h$ — высота изображения в словах;
$d_{\text{in}}$ — входная глубина изображения (количество входных карт признаков);
$d_{\text{out}}$ — выходная глубина изображения (количество выходных карт признаков).

Количество весов, которое необходимо прочитать при подобном подходе, составляет

$$S_{w1} = w_a h_a d_{\text{in}} d_{\text{out}}, \quad (2)$$

где $S_{w1}$ — суммарное количество весов для чтения (для удобства примем, что разрядности данных для обработки и весов совпадают);
$w_a$ — ширина окна свертки в словах;
$h_a$ — высота окна свертки в словах;
$d_{\text{in}}$ — входная глубина изображения;
$d_{\text{out}}$ — выходная глубина изображения.

Количество слов данных, которые необходимо прочитать для расчета выходного слоя вторым способом, составляет

$$S_{p2} = whd_{\text{in}}, \quad (3)$$

где $S_{p2}$ — суммарное количество слов данных для чтения;
$w$ — ширина изображения в пикселях;
$h$ — высота изображения в пикселях;
$d_{\text{in}}$ — входная глубина изображения.

Количество весов, которое необходимо прочитать при подобном подходе, составляет

$$S_{w2} = w_a h_a d_{\text{in}} d_{\text{out}} wh, \quad (4)$$

где $S_{w2}$ — суммарное количество весов для чтения;
$w_a$ — ширина окна свертки в пикселях;
$h_a$ — высота окна свертки в пикселях;
$d_{\text{in}}$ — входная глубина изображения;
$d_{\text{out}}$ — выходная глубина изображения;
$w$ — ширина изображения в пикселях;
$h$ — высота изображения в пикселях.

Очевидно, что в первом способе расчета необходимо больше транзакций с памятью для чтения входного изображения, но требуется меньше транзакций для чтения весов свертки. В случае второго способа расчета необходимо прочитать всего единожды входное изображение, однако необходимо при вычислении каждого выходного слова данных перечитывать все веса. При простой реализации (см. формулу) второй вариант требует значительно большего времени доступа к внешней памяти. Однако при небольшой глубине слоев можно сохранить в накристальной памяти сразу все веса, необходимые для вычисления текущего слоя, и тогда второй вариант становится менее затратным.

Для примера возьмем слой СНС, принимающий на входе изображения с размером 208×208 и глубиной 8, а на выходе — с размером 208×208 и глубиной 16 (табл. 1).

Таблица 1

**Сравнение двух вариантов вычисления слоя нейросети по требованию к пропускной способности к памяти**

| Вариант вычисления | Количество слов данных | Количество весов |
|---|---|---|
| 1 | 5537792 | 1152 |
| 2 | 346112 | 1152* |

* При условии, что все веса будут храниться в накристальной памяти.

Таким образом, при реализации второго варианта обработки можно сократить необходимую пропускную способность для чтения входного изображения слоя больше чем в 10 раз.

С увеличением глубины обрабатываемого слоя будет увеличиваться и количество весов, которые необходимо хранить в накристальной памяти. Для примера возьмем нейросеть YOLO. В табл. 2 приведены параметры нейросети (не описан последний слой с размером входных данных 13×13, входной глубиной 1024 и выходной глубиной 125,

т. к. он оказывает незначительное влияние на общее время обработки).

Таблица 2

**Параметры нейросети YOLO**

| Номер слоя | Размер изображения | Входная глубина | Выходная глубина |
|---|---|---|---|
| 1 | 416×416 | 3 | 16 |
| 2 | 208×208 | 16 | 32 |
| 3 | 104×104 | 32 | 64 |
| 4 | 52×52 | 64 | 128 |
| 5 | 26×26 | 128 | 256 |
| 6 | 13×13 | 256 | 512 |
| 7 | 13×13 | 512 | 1024 |
| 8 | 13×13 | 1024 | 1024 |

Примечание: при условии, что все веса будут храниться в накристальной памяти.

В табл. 3 приведено количество слов данных и весов, которые необходимо прочитать для расчета каждого слоя.

Таблица 3

**Сравнение первого и второго вариантов вычисления слоя нейронной сети по требованию к пропускной способности к памяти для всех слоев нейросети YOLO**

| Номер слоя | Вариант вычисления | Количество слоев данных | Количество весов | Суммарное количество данных |
|---|---|---|---|---|
| 1 | 1 | 8306688 | 432 | 8307120 |
| | 2 | 506688 | 432* | 507120 |
| 2 | 1 | 22151168 | 4608 | 22155776 |
| | 2 | 692224 | 4608* | 696832 |
| 3 | 1 | 22151168 | 18432 | 22169591 |
| | 2 | 346112 | 18432* | 364544 |
| 4 | 1 | 22151168 | 73728 | 22224896 |
| | 2 | 173056 | 73728* | 246784 |
| 5 | 1 | 22151168 | 294912 | 22446080 |
| | 2 | 86528 | 199360512** | —*** |
| 6 | 1 | 22151168 | 1179648 | 23330816 |
| | 2 | 43264 | 199360512** | —*** |
| 7 | 1 | 88604672 | 4718592 | 93323264 |
| | 2 | 86528 | 797442048** | —*** |
| 8 | 1 | 177209344 | 9437184 | 186646528 |
| | 2 | 173056 | 1594884096** | —*** |

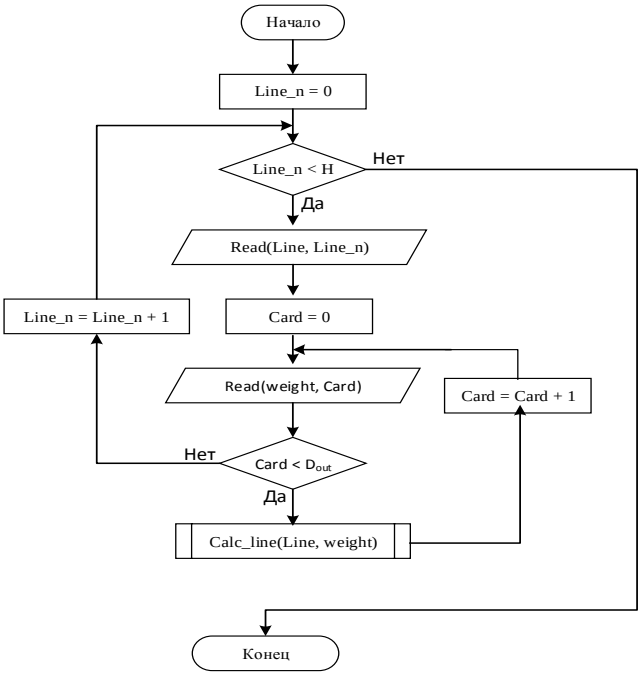
* При условии, что все веса будут храниться в накристальной памяти.

** Начиная со слоя 5 для второго варианта вычисления требуется слишком большое количество накристальной памяти для хранения всех весов (ни одна ПЛИС не содержит такого объема).

*** Расчеты не приведены, т. к. не имеют смысла ввиду отсутствия микросхем ПЛИС с достаточным объемом памяти.

Как видно из табл. 3, вычислять сразу все выходные карты признаков можно только до третьего-четвертого слоев нейросети (при проектировании нейросети YOLO; с другой нейросетью эти значения могут быть иными). Начиная с пятого слоя, требуется такое количество накристальной памяти, которое можно встретить только в старших микросхемах, и ее использование нецелесообразно.

При вычислении последующих слоев необходимо модифицировать второй способ обработки. Как уже было описано, второй способ обработки подразумевает вычисление всех карт признаков одновременно, но при этом требуется очень много накристальной памяти для хранения весов. Вместо этого необходимо производить обработку всех выходных слоев, но по одной строке отдельно для каждой выходной карты признаков (далее — третий способ вычисления). Алгоритм чтения данных представлен на рисунке.




***Алгоритм чтения данных при вычислении глубоких слоев СНС:***

Line_n — номер текущей обрабатываемой строки изображения; H — высота изображения в строках; Line — локальная память для хранения текущей строки; Read(Line, Line_n) — операция чтения строки с номером Line_n в локальную память; Card — номер выходной карты признаков; Weight — веса для формирования одной выходной карты признаков; Read(Weight, Card) — операция чтения весов соответствующих выходной карте признаков с номером Card; $D_{out}$ — глубина выходного изображения; Calc_line(Line, Weight) — вычисление выходной строки с использованием входной строки Line и весов Weight

Как видно из алгоритма, для вычисления выходного изображения потребуется прочитать входное изображение всего раз, но при этом необходимо несколько раз перечитывать веса. В табл. 4 приведено сравнение первого и третьего вариантов по требованию к пропускной способности внешней памяти при вычислении 5—8 слоев.

Таблица 4

**Сравнение первого и третьего варианта вычисления слоя нейронной сети по требованию к пропускной способности к памяти для 5—8 слоев нейросети YOLO**

| Номер слоя | Вариант вычисления | Количество слоев данных | Количество весов | Суммарное количество данных |
|---|---|---|---|---|
| 5 | 1 | 22151168 | 294912 | 22446080 |
| | 3 | 86528 | 7667712 | 7754240 |
| 6 | 1 | 22151168 | 1179648 | 23330816 |
| | 3 | 43264 | 15335424 | 15378688 |
| 7 | 1 | 88604672 | 4718592 | 93323264 |
| | 3 | 86528 | 61341696 | 61428224 |
| 8 | 1 | 177209344 | 9437184 | 186646528 |
| | 3 | 173056 | 122683392 | 122856448 |

Как видно из табл. 4, третий вариант вычисления экономичнее относится к пропускной способности внешней памяти. Суммарно при применении второго (до 4-го слоя включительно) и третьего (остальные слои) способов расчета слоя СНС можно получить экономию примерно в 50 %. При выборе другой нейросети слои, для которых следует применять второй или третий способ расчета, могут меняться.

### Выводы

Таким образом, применив второй и третий варианты расчета слоя СНС, расчет всех выходных карт признаков одновременно с хранением всех весов или только части весов, можно сократить необходимую пропускную способность внешней памяти примерно в 2 раза. Подобное уменьшение требований к пропускной способности памяти на встраиваемых системах (с низкой пропускной способностью) может увеличить скорость обработки до 2 раз. В зависимости от ситуации можно скомбинировать первый и третий варианты расчета, что позволит получить примерно 30%-й выигрыш в скорости.

**Литература**


1. *Беляков И. А.* Применение искусственных нейронных сетей при поиске уязвимостей в исходных текстах программного обеспечения // Изв. Петербургского университета путей сообщения. 2011. № 1. С. 120—129.
2. *Redmon J., Farhadi A.* YOLO9000: Better, Faster, Stronger. — University of Washington, Allen Institute for AI.
3. *Subarna T., Gokce D., Byeongkeun K., Vasudev B., Truong N.* LCDet: Low-Complexity Fully-Convolutional Neural Networks for Object Detection in Embedded Systems [Электронный ресурс]. Режим доступа: https://arxiv.org/abs/1705.05922.html (дата обращения: 25.09.2019).
4. *Courbariaux M., Bengio Y., David J.* Low precision arithmetic for deep learning [Электронный ресурс]. Режим доступа: https://arxiv.org/abs/1412.7024.html (дата обращения: 25.09.2019).
5. Официальная документация на контроллер внешней памяти ПЛИС ф. Altera [Электронный ресурс]. Режим доступа: https://www.altera.com/content/dam/altera-www/global/en_US/pdfs/literature/hb/external-memory/emi_plan.pdf (дата обращения: 25.09.2019).


## Optimisation of acces time to a dram for a compute neural net with FPGA


[1, 2] *A. S. Kushchenko,* [1] *O. B. Makarevich,* [1] *I. Yu. Polovko*

[1] Institute of Computer Technologies and Information Security, South Federal University, Taganrog, Rostov region, Russia

[2] JSC "Scientific Design Bureau of Computing Systems", Taganrog, Rostov region, Russia



*This article is dedicated to the study of the ways of discrete layers of convolution neural networks management calculation and abilities of an access to an external memory optimization as applied to the image processing. In this article is briefly described the most common approach of a calculation of a neural network layer and its disadvantage. As an alternative were proposed two approaches of a calculation that have advantages on different stages of a data processing with a neural network. An obtained method of a calculation of a convolution neural network layer allows significantly reduce the load of external memory. For an efficiency estimation were used theoretical calculations of the data size, which must be read from an external memory. There was made an estimation for work capability of FPGA with dynamic memory, such as DDR3 or DDR4. Usage of a dynamic memory is closer to the real condition than any other type of RAM, because it has a low cost and high capacity.*



*Keywords*: neural network convolution, FPGA, image processing, artificial intelligence.

Bibliography — 5 references.

*Received December 9, 2019*

# БЛАНК-ЗАКАЗ НА ПОДПИСКУ 2020 г.
# на издания ФГУП «НТЦ оборонного комплекса «Компас»

| Наименование издания | Индекс издания (количество выпусков в год) | Цена 1 экз., руб. | Кол-во выпусков в год | Общая сумма, руб. |
|---|---|---|---|---|
| Оборонный комплекс — научно-техническому прогрессу России | 79379 (4 вып.) | 1550,00 | | |
| Конструкции из композиционных материалов | 80089 (4 вып.) | 1700,00 | | |
| Экология промышленного производства | 80090 (4 вып.) | 1500,00 | | |
| Информационные технологии в проектировании и производстве | 79378 (4 вып.) | 1750,00 | | |
| Вопросы защиты информации | 79187 (4 вып.) | 1750,00 | | |
| *В цену включены: НДС — 10 % и стоимость почтовой доставки.* | | | | |

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

**Наши реквизиты:**

Полное наименование организации: _____

Сокращенное наименование организации: _____

ИНН/КПП _____

ОКПО _____

Расчётный счёт № _____ в _____

к/с _____ БИК _____

Юридический адрес: _____

Почтовый адрес: _____

Контактное лицо _____ тел. _____

E-mail: _____

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