ISSN 2074-7128(print), ISSN 2074-7136(on-line)

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
(IT Security)

Периодический рецензируемый научный журнал «Безопасность информационных технологий», освещающий широкий спектр проблем обеспечения информационной безопасности, в том числе технологические, организационно-правовые и образовательные аспекты.

Журнал зарегистрирован в Государственном комитете Российской Федерации по печати. Свидетельство №017789. Издается с 1994 г.

С момента основания и до настоящего времени учредителем журнала является федеральное государственное автономное образовательное учреждение высшего образования Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ).

С 2007 г. и по настоящее время журнал входит в Перечень ВАК ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук по отраслям науки и группе специальностей научных работников 05.13.00 – информатика, вычислительная техника и управление, по которой журнал входит в этот перечень.

Основные тематические направления журнала:
•Концептуальные основы обеспечения информационной безопасности автоматизированных систем;
•Методические подходы к анализу и оценке рисков информационной безопасности, технологии поиска уязвимостей в программном обеспечении;
•Оценка уровня защищенности автоматизированных систем;
•Программно-технические способы и средства обеспечения информационной безопасности.

Журналом приветствуются статьи на русском и английском языках.

IT Security(Russia)

IT Security is a periodic peer-reviewed scientific journal publishing papers on a wide range of information security topics, including technological, organizational, legal and educational problems.

Since its establishment in 1994 (registration certificate No. 017789 by the State Committee for Press of the Russian Federation), the journal has been publishing by the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University, a.k.a. "MEPhI" (Moscow Engineering Physics Institute).

Papers in Russian and English are equally welcome.

Focus topics:
•Fundamentals of information security of automated systems;
•Methodology of assessing the information security risks;
•Technology of detecting software vulnerabilities;
•Evaluation of the security level of automated systems;
•Soft- and hardware means of ensuring information security.

СОДЕРЖАНИЕ

CONTENT

Наталья Г. Милославская, Александр И. Толстой
Национальный исследовательский ядерный университет «МИФИ»
115409, Москва, Каширское шоссе, 31, Россия
e-mail: NGMiloslavskaya@mephi.ru, ORCID 0000-0002-1231-1805
e-mail: AITolstoj@mephi.ru, ORCID 0000-0001-9265-1510

КОМПЕТЕНТНОСТНЫЕ ТРЕБОВАНИЯ СТАНДАРТОВ ISO/IEC К ПРОФЕССИОНАЛАМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2017.4.01

Аннотация. Наша динамичная жизнь поставила нас перед необходимостью периодической коррекции разработанных в настоящее время профессиональных компетенций (сформулированы в федеральных государственных образовательных стандартах) и трудовых функций (сформулированы в профессиональных стандартах) для очень популярной области информационной безопасности (ИБ). В таких условиях чрезвычайно важным является своевременная реакция на все новое, которое появляется или будет появляться в современных нормативных документах (прежде всего в стандартах). В данной работе сделан прогноз содержания разрабатываемой международной организацией стандартизации (ISO) проектов стандартов ISO/IEC 27021 и ISO/IEC 19896, которые должны содержать требования к компетентности профессионалов в области систем менеджмента ИБ и к компетентности тестировщиков и оценщиков ИБ. Прогноз сделан с учетом требований, содержащихся в группе стандартов ISO/IEC 27000 и рекомендаций документа «Европейская модель электронной компетентности e-CF 3.0».

Ключевые слова: информационная безопасность, компетентность, профессионал в области информационной безопасности, стандарт ISO/IEC.

Для цитирования. **МИЛОСЛАВСКАЯ, Наталья Г.; ТОЛСТОЙ, Александр И.** КОМПЕТЕНТНОСТНЫЕ ТРЕБОВАНИЯ СТАНДАРТОВ ISO/IEC К ПРОФЕССИОНАЛАМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 6-18, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/282>. Дата доступа: 28 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.01.

Natalia G. Miloslavskaya, Alexander I. Tolstoy
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: NGMiloslavskaya@mephi.ru, ORCID 0000-0002-1231-1805
e-mail: AITolstoj@mephi.ru, ORCID 0000-0001-9265-1510

Competence Requirements of ISO/IEC Standards for Information Security Professionals

DOI: http://dx.doi.org/10.26583/bit.2017.4.01

Abstract. The rapid progress in the filed of information security (IS) puts one in a need of periodic revision of professional competencies (formulated in the federal state educational standards –FSESs) and working functions (formulated in the professional standards – PSs). Under these conditions, a timely reaction to everything new that emerges or will appear in modern regulatory documents (primarily in standards) is extremely important. We make a forecast for the content of the ISO/IEC 27021 and ISO/IEC 19896 standards drafted by the International Organization for Standardization (ISO), which should contain the requirements for the competencies of IS management system professionals and the competence of IS testers and evaluators. Our forecast takes into account the requirements of the ISO/IEC 27000 standard group and the recommendations of the European e-Competence Framework e-CF 3.0.

Keywords: information security, competence, Information Security Professional, ISO/IEC standard

For citation. **MILOSLAVSKAYA, Natalia G.; TOLSTOY, Alexander I.** Competence Requirements of ISO/IEC Standards for Information Security Professionals. IT Security, [S.l.], v. 24, n. 4, p. 6-18, nov. 2017. ISSN 2074-

7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/282>. Date accessed: 28 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.01.

Введение

В настоящее время наблюдается растущая потребность в профессиональных кадрах в быстро развивающейся области информационной безопасности (ИБ). Современный подход к определению квалификационных требований к таким кадрам основан на формулировании профессиональных компетенций (далее компетенций) как способности решать поставленные задачи и выполнять определенную работу в рамках профессиональной деятельности[1].

В Российской Федерации квалификационные требования к профессиональным кадрам сформулированы в двух группах нормативных документов:

1. Федеральные государственные образовательные стандарты (ФГОС) – в виде компетенций (общекультурных, общепрофессиональных и профессиональных) для выпускников образовательных учреждений. ФГОСы утверждены приказами Министерства образования и науки РФ. По направлению «Информационная безопасность» в области высшего образования действуют ФГОСы для семи специальностей (специалитет) и для трех направлений (бакалавриат, магистратура и аспирантура).

2. Профессиональные стандарты (ПС) – в виде трудовых действий, которые должны выполнять профессионал, имеющий определенный образовательный уровень и занимающий определенную должность. По направлению «Информационная безопасность» действуют три профессиональных стандарта, утвержденные приказами Министерства труда и социальной защиты РФ.

Необходимо отметить, что межведомственная несогласованность не позволила выработать единый подход к выбору общей методологической базы оценки квалификационного уровня. Это привело к тому, что в образовательной сфере при формулировании профессиональных компетенций необходимо находить соответствия между профессиональными компетенциями (ФГОС) и трудовыми функциями (ПС). В этом случае такое соответствие возможно установить через сравнение характеристик (параметров или атрибутов), относящихся к профессиональным компетенциям (требования к знаниям (З), умениям (У) и навыкам (Н)) и к трудовым действиям (требования к знаниям и умениям). Соответствующие характеристики должны быть определены в основной образовательной программе, относящейся к определенному ФГОСу (З, У, Н), и сформулированы в профессиональных стандартах (З, У).

Следует ожидать, что в будущем при модернизации образовательных и профессиональных стандартов будут предприняты шаги по смягчению указанной выше несогласованности. При этом представляется полезным учесть опыт формулирования квалификационных требований, накопленный на международном уровне.

Усилия по разработке общего подхода к формулированию требований к компетенциям в области ИБ ведутся во всем мире в течение длительного времени. На начальном этапе была сделана попытка описать необходимый объем знаний (НОЗ) как «набор структурированной информации, которая создает основу для понимания терминов и компетенций в определенной области знаний» [2]. НОЗ относится только к первой компоненте отдельной компетенции (З). Первые попытки выработать общую точку зрения по этому вопросу в целом относятся к международным конференциям по обучению в области ИБ (World international conferences on IS Education – WISE) конца 1990-х – начала 2000-х годов [3-5]. Одновременно с этим для целей сертификации специалистов в области безопасности были разработаны несколько описаний НОЗ для практиков (типа CISA, CISSP, GIAC и т.д.).

В настоящее время можно констатировать, что сформировались три базовых подхода:

1. Американский – в нормативных документах, разработанных Национальным подразделением кибербезопасности Департамента национальной безопасности США: «Необходимый объем знаний для защиты информационных технологий (ИТ): компетентность и функциональная модель подготовки кадров в области ИТ» [7] и более специализированная «Национальная инициатива по образованию в области кибербезопасности» [8];

2. Австралийский – в нормативном документе Офиса информационного менеджмента при Правительстве Австралии (AGIMO) «Модель умений в области кибербезопасности и карта ролей в области ИБ» [9];

3. Европейский – в нормативном документе Европейской Комиссии «Европейская модель электронной компетентности e-CF 3.0» [10].

Ожидается, что данный опыт будет обобщен и использован (особенно в отношении документа e-CF 3.0) в новых международных стандартах Международной организации по стандартизации (ИСО):

- ISO/IEC 27021 «Информационные технологии – Методы и средства обеспечения безопасности – Требования к компетентности специалистов в области систем менеджмента информационной безопасности»;
- ISO/IEC 19896 «Информационные технологии – Требования к компетентности для тестировщиков и оценщиков информационной безопасности» (три части):
  - «Введение, термины и общие требования»;
  - «Требования к знаниям, навыкам и эффективности для тестировщиков в соответствии с ISO/IEC 19790»;
  - «Требования к знаниям, навыкам и эффективности для оценщиков в соответствии с ISO/IEC 15408».

Данная статья анализирует основные положения документа e-CF 3.0, а также содержит прогноз возможного содержания стандартов ISO/IEC 27021 и ISO/IEC 19896.

1 Европейская модель электронной компетентности

Третья версия Европейской модели электронной компетентности (e-CF 3.0) [10] является результатом десяти лет работы многих заинтересованных сторон из европейского сектора информационно-коммуникационных технологий (ИКТ), при поддержке Европейской Комиссии и при тесном сотрудничестве с сообществом CENICTSkills Workshopcommunity. Термин «электронная» указывает на отношение компетенций к определенной области профессиональной деятельности – ИКТ. Этот объемный документ определяет компетентность как демонстрируемое умение (У)применять знания (З) и навыки (Н) и соответствующее отношение для достижения наблюдаемых результатов. Умение – это способность выполнять физические или умственные действия, которые связаны с той или иной профессии. Знание – это узнавание фактов, истин и принципов, полученных в процессе традиционного обучения и/или опыта. Навык – это развитая ловкость или сноровка в осуществлении умственных операций или физических процессов, которые часто приобретаются посредством специализированного обучения (использование этих навыков приводит к успешной работе). Способность применять знания и навыки продуктивным образом также можно дополнительно охарактеризовать такими признаками поведения, как, например, инициатива, энтузиазм, желание, навыки общения, работа в команде, руководство и других. Все это в совокупности показывает эффективность деятельности профессионала в определенной области, что определяет уровень его компетентности.

Для того, чтобы описать компетентность профессионала в области ИКТ документ e-CF 3.0 предлагает воспользоваться четырьмя группами характеристик, отражающими

разные уровни требований бизнеса и планирования людских ресурсов (в дополнение к знанию принципов исполнения должностных обязанностей/работы):

Группа 1: определяет пять видов профессиональной деятельности, относящихся к основным процессам ИКТ: Планирование (A) – Создание (B) – Выполнение (C) – Обеспечение (D) – Управление (E).

Группа 2: содержит формулировки профессиональных компетенций (их в e-CF 3.0 приведено 40) для каждого вида профессиональной деятельности из Группы 1.

Группа 3: определяет уровни владения для каждой профессиональной компетенции из Группы 2.

Группа 4: формулирует перечень знаний и навыков (к сожалению, без умений) для каждой профессиональной компетенции из Группы 2.

Основным недостатком документа e-CF 3.0 является то, что он содержит общее описание уровня компетентности только для двух типов профессионалов в области ИБ, относящихся к ИКТ, а именно Администратора безопасности ИКТ и Специалиста по безопасности ИКТ. Для удобства сравнения эти описания были сведены в единую таблицу (табл.1). Миссией Администратора безопасности ИКТ является управление политикой безопасности ИКТ (ПБИКТ), а миссией Специалиста по безопасности ИКТ – обеспечение выполнения ПБИКТ на объекте. В соответствии с этим определены их функциональные обязанности в виде основных задач и ожидаемых результатов деятельности. При этом ключевыми показателями эффективности их деятельности соответственно являются эффективность ПБИКТ и работоспособные меры защиты.

Таблица 1. Общее описание уровня компетентности Администратора безопасности ИКТ и Специалиста по безопасности ИКТ

Администратор безопасности ИКТ	***Специалист по безопасности ИКТ***
Миссия: Управляет политикой безопасности ИКТ (ПБИКТ). • Определяет ПБИКТ. • Управляет развертыванием защитных мер для всех ИС. • Обеспечивает предоставление доступа к информации. • Выступает в качестве эксперта по ПБИКТ, признаваемого внутренними и внешними заинтересованными сторонами.	***Миссия:*** Обеспечивает выполнение ПБИКТ на объекте. • Предлагает и реализует необходимые обновления мер защиты. • Консультирует, поддерживает, информирует и обеспечивает обучение и осведомленность в области безопасности. • Осуществляет непосредственные действия в отношение всей или части сети или системы. • Выступает в качестве эксперта по технической защите ИКТ, признаваемого сослуживцами.
Результаты работы: • *базовые (учетные):* ПБИКТ; • *в зоне ответственности:* База знаний или Информационная база, Стратегия обеспечения ИБ (ОИБ); • *в зоне совместной работы с другими исполнителями:* Политика управления рисками, Предложения по интеграции новых технологий, Стратегия и реализация ИКТ.	***Результаты работы***: • *базовые (учетные):* База знаний или Информационная база (в области ИБ); • *в зоне ответственности:* Предложения по интеграции новых технологий (в области ИБ); • *в зоне совместной работы с другими исполнителями:* Политика и план управления рисками, ПБИКТ.
Основные задачи: • определяет и реализует процедуры, связанные с безопасностью ИКТ; • способствует разработке политики безопасности организации; устанавливает план профилактики; • информирует и повышает осведомленность среди общего руководства; • обеспечивает продвижение идей безопасности ИТ среди пользователей; • проверяет и поддерживает применение принципов и правил ОИБ.	***Основные задачи:*** • обеспечивает безопасность и надлежащее использование ресурсов ИКТ; • оценивает риски, угрозы и последствия; • обеспечивает тренинги и подготовку в области ИБ; • обеспечивает техническую проверку средств защиты; • способствует использованию стандартов безопасности; • проводит аудит уязвимостей; • следит за разработками в области безопасности, что обеспечивает защиту данных и физическую защиту ресурсов ИКТ.

Ключевые показатели эффективности: эффективность ПБИКТ.	***Ключевые показатели эффективности:*** соответствующие работоспособные меры защиты.

В e-CF 3.0 общее описание уровня компетентности дополнено перечнем и описанием профессиональных компетенций с указанием соответствующих им уровней владения (УВ). Фрагменты таких описаний приведены в табл.2 для Администратора безопасности ИКТ и в табл.3 для Специалиста по безопасности ИКТ соответственно.

Таблица 2. Описание профессиональных компетенций для Администратора безопасности ИКТ

Профессиональная компетенция, относящаяся к определенному виду профессиональной деятельности, и ее описание	**Уровень владения профессиональной компетенцией**
A.7.Мониторинг новых технологий (способен): • исследовать последние технологические разработки в области ИКТ для формирования единого понимания новых технологий; • интегрировать новые технологии в существующие продукты, приложения или сервисы; • разрабатывать инновационные решения для выработки новых решений.	УВ.4: • использует широкие знания новых и развивающихся технологий, в сочетании с глубоким пониманием бизнеса для осмысления и выработки решений на перспективу: • руководит командой в качестве эксперта и консультирует ее для поддержки принятия стратегических решений.
D.1.Разработка стратегии ОИБ (способен): • определять и делать реализуемыми в организации формализованную стратегию, границы и культуру обеспечения безопасности и защищенности информации от внешних и внутренних угроз; • применять методы компьютерной форензики для корпоративных расследований или расследования вторжений; • создавать основу для управления ИБ, в том числе за счет определения и установления подотчетности ролей; • применять надлежащие стандарты для определения целей обеспечения целостности, доступности и конфиденциальности данных.	УВ.5: • обеспечивает стратегическое руководство при встраивании ИБ в культуру организации.
E.3.Управление рисками (способен): • осуществлять управление рисками посредством применения установленных в организации политики и процедур управления рисками для информационных систем; • оценивать риски для бизнеса организации, в том числе для сети, облачных вычислений и мобильных ресурсов; • документировать потенциальные риски и планы их обработки.	УВ.3: • принимает решение о соответствующих действиях, необходимых для адаптации подходов к обеспечению безопасности и установлению риска безопасности; • оценивает, управляет и обеспечивает проверку исключений; проводит аудит процессов и среды в области ИКТ.
E.8.Управление ИБ (способен): • реализовывать политику ОИБ; • осуществлять мониторинг и принимать меры против вторжений, мошенничества и нарушения безопасности или утечек; • гарантировать, что риски безопасности для корпоративных данных и информации анализируются и управляются; • анализировать инциденты безопасности, формулировать рекомендации по политике и стратегии ИБ, обеспечивающие ее непрерывное совершенствование.	УВ.4: • руководит обеспечением целостности, конфиденциальности и доступности данных, хранящихся в информационных системах, и соблюдением соответствия всем требованиям законодательства.
E.9.Руководство ИБ (способен): • определять, разворачивать и контролировать управление ИБ информационных систем в соответствии с бизнес-требованиями; • учитывать все внутренние и внешние параметры, такие как	УВ.4: • руководит стратегией управления ИБ посредством обмена информацией,

соответствие законодательству и стандартам (что влияет на управление рисками и распределение ресурсов) для достижения сбалансированного успеха бизнеса.	распространения и контроля соответствующих процессов во всей инфраструктуре ИКТ.

Таблица 3. Описание профессиональных компетенций для Специалиста по безопасности ИКТ

Профессиональная компетенция, относящаяся к определенному виду профессиональной деятельности, и ее описание	**Уровень владения профессиональной компетенцией**
C.2.Поддержка изменений (способен): • реализовывать и направлять эволюцию решений в области ИКТ; • обеспечивать эффективный контроль и планирование программных или аппаратных модификаций для предотвращения множественных обновлений, создающих непредсказуемые результаты; • сводить к минимуму нарушения предоставления услуг вследствие изменений и придерживает определенный соглашением уровень обслуживания (SLA); • обеспечивать рассмотрение и соблюдение процедур ОИБ.	УВ.3: • обеспечивает целостность систем, контролируя установку функциональных обновлений, программных или аппаратных дополнений и работ по техническому обслуживанию; • соблюдает требования бюджета.
C.3.Предоставление услуг (способен): • обеспечивать предоставление услуг в соответствии с установленным SLA; • предпринимать активные действия по обеспечению стабильной работы и защите приложений и инфраструктуры ИКТ для избегания потенциальных нарушений обслуживания, связанных с планированием производственных мощностей и ИБ; • обновлять библиотеку операционной документации и регистрирует все инциденты нарушения работы сервисов; • поддерживать работу средств мониторинга и управления (ПО, процедуры); • предоставлять услуги в области ИБ; • предпринимать упреждающие меры.	УВ.3: • устанавливает график выполнения оперативных задач; • управляет расходами и бюджетом в соответствии с внутренними процедурами и внешними ограничениями; • определяет оптимальное число сотрудников, необходимых для обеспечения оперативного управления инфраструктурой ОИБ.
D.9.Повышение квалификации персонала (способен): • диагностировать компетентность отельных лиц и групп, определяя потребности и нехватку квалификации; • анализировать предложения по обучению и повышению квалификации и выбирать соответствующую методику с учетом требований отдельных лиц, проектов и бизнеса; • проводить тренинги и/или выступать наставником отдельных лиц и групп для удовлетворения потребностей в обучении.	УВ.3: • осуществляет мониторинг и решает вопросы повышения квалификации людей и групп.
D.10.Управление информацией и знаниями (способен): • определять и управлять структурированной и неструктурированной информацией и предлагать политику распространения информации; • создавать информационную структуру для использования и оптимизации информации; • понимать работу соответствующих средств, которые будут внедрены для создания, извлечения, поддержания, обновления и распространения бизнес-знаний, преумножающих капитал за счет информационных активов.	УВ.3: • анализирует бизнес-процессы и связанные с ними требования к информации и предусматривает наиболее подходящую информационную структуру.
E.8.Управление ИБ (способен): Как для Администратора безопасности ИКТ.	УВ.3: • оценивает меры и показатели управления безопасностью и решает вопросы их соответствия политике ОИБ; • исследует и активизирует меры по устранению каких-либо нарушений безопасности.

	УВ 4: Как для Администратора безопасности ИКТ.

Анализ приведенных данных позволяет сделать следующие выводы:

1. Администратор безопасности ИКТ и Специалист по безопасности ИКТ имеют или разные, или общие виды профессиональной деятельности.

2. К разным видам профессиональной деятельности относятся Планирование (A) для Администратора безопасности ИКТ в части профессиональной компетенции A.7.Мониторингновых технологий, а для Специалиста по безопасности ИКТ – Выполнение(C) в отношении профессиональных компетенций C.2.Поддержка изменений и C.3.Предоставление услуг.

3. К общим видам профессиональной деятельности относятся Обеспечение (D) и Управление (E) со своими профессиональными компетенциями: D.1.Разработка стратегии ОИБ, E.3.Управление рисками, E.8. Управление ИБ и E.9.Руководство ИБ (для Администратора безопасности ИКТ); (способен): D.9.Повышение квалификации персонала, D.10.Управление информацией и знаниями, E.8.Управление ИБ (для Специалиста по безопасности ИКТ).

4. Имеется общий вид профессиональной деятельности Управление (E) с одинаковой профессиональной компетенцией E.8.Управление ИБ, одинаковым ее описанием и уровнем владения УВ.4.

Be-CF 3.0 определены характеристики (параметры или атрибуты), относящихся к профессиональным компетенциям в виде требований к знаниям (З, в тексте документа - K) и навыкам (Н, в тексте документа - S). Например, Для профессиональной компетенции У.8.Управление ИБ приведено семь характеристик «знание» (K1, …, K7) и семь характеристик «навыки» (S1, … ,S7). Приведем их примеры.

Профессионал должен знать: особенности построения политики управления ИБ объекта и ее использования при взаимодействии с клиентами, поставщиками и субподрядчиками (K1); лучшие практики и стандарты в области управления ИБ (K2); критические риски для управления ИБ (K3); подходы к внутреннему аудиту ИКТ (K4); методы определения ИБ, в том числе мобильных устройств (K5); методы кибератак и меры противодействия для их предотвращения (K6); методы компьютерной форензики (K7).

Профессионал должен обладать следующими навыками: документирования политики управления ИБ с учетом связи с бизнес-стратегией организации(S1); проведения анализа критически важных активов организации и выявления слабых мест и уязвимостей для вторжений или атак(S2); разработки плана управления рисками для обеспечения и выполнения плана превентивных действий(S3); проведения аудитов ИБ (S4); применения методов мониторинга и тестирования(S5); создания плана восстановления(S6); реализации плана восстановления в случае кризиса (S7).

Следует отметить, что отдельные характеристики «знание» и отдельные характеристики «навыки», имеющие отношение к области ИБ, в e-CF 3.0 сопоставлены с другими профессиональными компетенциями, сформулированными для профессионалов, миссия которых не связана непосредственно с обеспечением ИБ ИКТ: для профессиональной компетенции A.1. Выравнивание стратегии бизнеса и ИС необходимы *знания в области ИБ* (K8) и навыки в *развитии стратегии и политики в области ИКТ, включая безопасность и качество ИКТ* (S4);для A.2. Управление уровнем обслуживания необходимы знания *стандартов безопасности для ИКТ* (K6);для A.5. Архитектурный дизайн необходимы знания требований к архитектуре систем (производительность, ремонтопригодность, расширяемость, масштабируемость, доступность, *безопасность*) и *управление доступом* (K2);для B.1 Разработка приложений необходимы знания *основ ИБ*(K14);для C.2. Поддержка изменений и C.3. Предоставление услуг необходимы знания *лучших практик и стандартов в управлении ИБ* (K5).

Анализ документа e-CF 3.0 в целом позволяет сделать вывод о том, что описание профессиональных компетенций в области ИБ не является основной целью этого документа. Поэтому он может быть использован лишь как наиболее общее начальное руководство, требующее дальнейших существенных дополнений и уточнений.

2 Чего ожидать от ISO/IEC 27021

Признанная среди профессионалов серия международных стандартов ISO/IEC 27000 как сборник лучших практик в области менеджмента ИБ в скором времени будет расширена новым стандартом ISO/IEC 27021 «Информационная технология – Методы и средств обеспечения безопасности – Требования к компетентности специалистов в области систем менеджмента информационной безопасностью». Его разработка была начата осенью 2013 г., а публикация объявлена на осень 2017 г. (в июле 2017 г. он находился на стадии разработки 50.00 “Получен окончательный текст или Финальный проект стандарта зарегистрирован для одобрения”). Предоставляя НОЗ только в узконаправленной области управления, а также определяя необходимые умения и т.п. для специалистов, этот стандарт, как ожидается, будет содержать описание минимальных квалификационных требований к профессионалам, имеющих отношение к созданию, внедрению, поддержанию и постоянному совершенствованию системы менеджмента ИБ (СМИБ) в соответствии с циклом PDCA (Plan-Do-Check-Act).

Статья 7.2 основного из серии стандарта ISO/IEC 27001, гармонизированного в Российской Федерации до уровня национального стандарта ГОСТ Р ИСО/МЭК 27001, требует поддержки СМИБ компетентными кадрами [11]. Для выполнения выше указанного требования должны быть реализованы следующие мероприятия: определение квалификационных требований к профессионалам, которые имеют отношение к обеспечению ИБ в организации и на объектах (с учетом накопленного опыта эти требования, скорее всего, будут сформулированы в виде необходимых профессиональных компетенций); формирование этих профессиональных компетенций у персонала организации, который не отвечает предъявляемым организацией квалификационным требованиям по обеспечению ИБ; подбор кадров при приеме на работу с учетом квалификационных требований; оценка эффективности любых мер, направленных на приобретение сотрудниками организации необходимой профессиональных компетенций в области ИБ; проведение аттестации профессионалов в области ИБ.

Потенциальная целевая аудитория стандарта ISO/IEC 27021 может включать в себя, следующие категории, но не ограничивать ими:

а) организации, ищущие профессионалов в области менеджмента ИБ для занятия определенных должностей для себя, или кадровые агентства для отбора профессионалов в области менеджмента ИБ для занятия определенных должностей в организациях – заказчиках подобных кадров. Профессиональные компетенции из этого стандарта позволят осуществить необходимый отбор;

б) образовательные учреждения, ведущие подготовку кадров в области ИБ. Квалификационные требования из стандарта позволят сориентировать основные образовательные программы подготовки профессионалов различного уровня в части конечного результата их деятельности;

в) сертификационные центры как независимые органы оценки квалификационного уровня специалистов в области ИБ;

г) профессионалы, которые определяют направления повышения своей квалификации с учетом требований рынка труда;

д) студенты для понимания и получения тех компетенций, которые необходимы в их дальнейшей работе.

Из анализа стандарта ISO/IEC 27001 можно сделать вывод, что все квалификационные требования к профессионалам в области менеджмента ИБ скорее всего будут разделены на три группы: общие (не зависящие от предметной области), предметно-

ориентированные в области ИБ и предметно-ориентированные в области менеджмента ИБ. Некоторые примеры предметных областей, для которых возможно будут описаны квалификационные требования по группам:

1) общие:

- Базовые: дизайн, лидерство, стратегии и политики, культура и бизнес организации, финансы и бюджет;
- Управление: основы управления: управление проектами, управление проблемами, управление взаимоотношениями с поставщиками, управление людскими ресурсами, аналитические методы, измерение эффективности и результативности, соответствие;
- Информационные технологии: ИКТ, информационные системы, связь;

2) Предметно-ориентированные в области ИБ:

- Управление ИБ в рамках управления бизнесом: бизнес-контекст организации, концепции управления, стратегии, стандарты в области ИБ (на базе ISO/IEC 27014) и политики, специфичные для СМИБ правовые и нормативные вопросы, методологии оценки ИБ, обеспечение непрерывности бизнеса, управление активами и т.д.;
- Управление рисками ИБ: оценка и обработка рисков ИБ и их применение в рамках СМИБ (на базе ISO/IEC 27005);
- Управление инцидентами ИБ: обнаружение, отчетность, оценка и реагирование на инциденты ИБ, их применение в рамках СМИБ (на базе ISO/IEC 27035);
- Аудит ИБ: внутренний и внешний аудит ИБ, мониторинг и самооценка, их применение в рамках СМИБ (на базе ISO/IEC 27006-2708);
- Средства управления ИБ: реализация правил политик ИБ, контроль доступа, криптография, безопасность функционирования и связи, безопасность кадровых ресурсов, физическая и экологическая безопасность, безопасность систем, соответствие и т.д.

3) Предметно-ориентированные компетенции в области СМИБ:

- Планирование СМИБ: анализ влияния на бизнес, активы, критерии принятия рисков ИБ, средства управления ИБ, моделирование угроз, управление уязвимостями, защитные меры, стратегия и политика ОИБ, сфера применения СМИБ, цели, структура, роли;
- Функционирование СМИБ: проектирование подпроцессов ОИБ, внедрение, эффективное и результативное функционирование и документация, мониторинг ИБ, системы обнаружения и предотвращения вторжений, контроль доступа, антивирусное программное обеспечение, системный журнал, SIEM-системы, управление конфигурированием и исправлениями;
- Поддержка СМИБ: жизненный цикл подпроцессов СМИБ, документация, повышение осведомленности, обучение и профессиональная подготовка, система управления обучением;
- Оценка эффективности СМИБ: аудит, мониторинг, измерение и анализ ИБ, соблюдение соответствия с внешними/внутренними нормативными актами;
- Совершенствование СМИБ: постоянное стратегическое и тактическое улучшение всех ключевых аспектов СМИБ в соответствии с самыми последними технологическими инновациями и методологиями.

3 Чего ожидать от ISO/IEC 19896

Стандарт ISO/IEC 19896 «Информационные технологии – Требования к компетентности для тестировщиков и оценщиков информационной безопасности» разрабатывается в трех частях.

Стандарт ISO/IEC 19896-1 «Введение, термины и общие требования» будет определять условия и устанавливать организованный набор понятий и отношений для квалификационных требований в области ИБ к специалистам по оценке обеспечения безопасности ИТ-продуктов и проверке их на соответствие, а также к специалистам-тестеровщикам безопасности ИТ-продуктов для проведения их тестирования/оценки с

использованием стандартов, разрабатываемых Комитетом ИСО по оценке соответствия (Committee on Conformity Assessment, CASCO). Первая часть стандарта ISO/IEC 19896 содержит базовую информацию для понимания требований, включенных в следующие части этого стандарта. По сравнению с проектом ISO/IEC 27021, проект ISO/IEC 19896-1 находится на стадии 40.20 “Инициировано голосование по проекту стандарта” на июль 2017г. Его потенциальная целевая аудитория может включать специалистов (тестировщиков и оценщиков), проводящих оценку и контроль соответствия ИБ и продуктов ИБ, валидаторов, органы сертификации и утверждения, испытательные лаборатории, продавцов и технических поставщиков, а также организации, предлагающие профессиональную сертификацию.

СтандартISO/IEC 19896-2 «Требования к знаниям, навыкам и эффективности для тестировщиков в соответствии с ISO/IEC 19790» будет содержать формулировки минимальных требований к уровню знаний и навыков для лиц, проводящих испытания и оценку в соответствии рекомендациями стандартов ISO/IEC19790 «Информационная технология – Методы и средства обеспечения безопасности – Требования безопасности для криптографических модулей».

Стандарт ISO/IEC 19896-3 «Требования к знаниям, навыкам и эффективности для оценщиков в соответствии с ISO/IEC 15408» будет содержать формулировки минимальных требований к уровню знаний и навыков для лиц, проводящих оценку в соответствии с рекомендациями стандарта ISO/IEC 15408 «Информационная технология – Методы и средства обеспечения безопасности – Критерии оценки безопасности информационных технологий».

Без сомнений все три части нового стандарта ISO/IEC 19896 будут основываться на стандарте ISO/IEC 17025«Общие требования к компетентности испытательных и калибровочных лабораторий», который также был подготовлен комитетом ИСО CASCO и устанавливает общие требования к компетентности широкого круга лабораторий в проведении испытаний и/или калибровки (не только в области проверки и оценки ИТ-продуктов с точки зрения ОИБ). В пятом разделе ISO/IEC 17025:2005 приводятся два требования: руководство лаборатории должно гарантировать компетентность всех, кто работает со специальным оборудованием, проводит испытания и/или калибровки, оценивает результаты и подписывает протоколы испытаний и сертификаты о калибровке, а также то, что специфические задачи следует поручать персоналу с учетом соответствующего образования, подготовки, опыта и/или проявляемого мастерства. Таким образом, в целях поддержки соответствия при оценке или проверке соответствия обеспечения безопасности ИТ-продуктов, одним из ключевых факторов является компетентность лиц, выполняющих эту работу. Что же касается любой другой профессиональной деятельности, то для поддержки достижение соответствия и повторяемости результатов необходима минимальная компетентность. Основными элементами компетентности являются минимально необходимые знания, навыки, опыт и квалификация, соответствующие целевому стандарту обеспечения безопасности ИТ-продуктов.

Квалификационные требования (профессиональные компетенции и их характеристики – У, З, Н) в этом случае формируется из знания архитектуры и дизайна ИТ-продукта в соответствующих технологических областях, всех применимых стандартов, политик и процедур, любых связанных с ними методов испытаний или оценок, типичных уязвимостей, которые могут возникнуть в этом продукте или технологии. Навыки означают способность понимать область оценки и тестирования (их границы), анализировать различную документацию, понимать исходный код, используемый в специфицированных и реализованных продуктах, разрабатывать и выполнять функциональные и специальные процедуры тестирования ИБ, использовать специализированные инструменты тестирования, интерпретировать результаты тестирования и писать отчеты, детализирующие эти результаты. Дополнительные навыки эффективного общения и выполнения управления проектами необходимы на более

высоких уровнях компетентности. При этом важным является накопленный опыт проведения оценки или тестирования и, возможно, наставнической деятельности.

Спецификация конкретных образовательных квалификаций может помочь определить способность человека следовать формальной программе или работать независимо друг от друга. В некоторых случаях приемлемо заменить образование или квалификацию соответствующим опытом.

Эти основные элементы компетенции могут быть расширены с помощью некоторых дополнительных элементов, таких как лидерство, работа в команде, инициативность, способности, желания и так далее.

Все характеристики, определяющие квалификационный уровень, должны быть измеряемы. Уровень профессиональной квалификации может быть определен на основе документа (сертификата), выданного образовательным учреждением. При необходимости провести измерение таких характеристик, как знание (З) и навыки (Н), можно использовать методы тестирования по программам, учитывающим требования, сформулированные в соответствующих нормативных документах, таких, как, например, рассматриваемый стандарт. Методы и программы измерения характеристик могут быть ориентированы на требования отдельных организаций (лабораторий), если речь идет о персонале, который работает или претендует на работу в этой организации. Опыт должен измеряться не годами работы на определенных должностях, а количеством проектов, в которых профессионал участвовал до этого (с учетом сложности проекта, используемых технологий и методов испытаний).

Может быть обоснованным включить в ISO/IEC 19896-1 несколько квалификационных уровней, которые могут соответствовать разным уровням профессиональной способности, а также позволяют определять профессиональные роли в организациях и связать их с конкретными профессиональными компетенциями. Например, первый уровень (техник) поддерживает работу профессионалов, относящихся к более высоким уровням. Второй уровень участвует в тестировании под соответствующим руководством. Третий уровень (оценщик или тестировщик) компетентен работать без руководства во многих случаях, но может потребоваться наблюдения и контроля. Четвертый уровень (ведущий оценщик или тестировщик) компетентен работать без руководителя во всех областях тестирования или оценки в соответствии с определенными стандартами и методами, способен обеспечивать управление проектами, руководить работой сотрудниками, относящимся к предыдущим уровням, и общаться с заинтересованными сторонами.

Заключение

Наша динамичная жизнь поставила нас перед необходимостью периодической коррекции разработанных в настоящее время профессиональных компетенций (сформулированы в федеральных государственных образовательных стандартах) и трудовых функций (сформулированы в профессиональных стандартах) для очень популярной области ИБ. В таких условиях чрезвычайно важным является своевременная реакция на все новое, которое появляется или будет появляться в современных нормативных документах (прежде всего в стандартах). В данной статье предпринята попытка прогноза содержания разрабатываемой ИСО проектов стандартов ISO/IEC 27021и ISO/IEC 19896-1. Представленный прогноз основывается на двух предпосылок:

1. При формулировании квалификационных требований необходимо учитывать современные требования по ОИБ, которые изложены в группе стандартов ISO/IEC 27000 и которые отражают современный подход, базирующийся на утверждении, что эффективность ОИБ определяется эффективностью управления процессами ОИБ.

2. Описание квалификационных характеристик должно строиться на компетентностном подходе на основе формулирования профессиональных компетенций и

связанных с ними групп характеристик «знания», «умения» и «навыки». Основы этого подхода изложены в европейском документе e-CF 3.0.

В сделанном прогнозе содержания стандартов ISO/IEC 27021 и ISO/IEC 19896-1 важное место занимает не только формулирование квалификационных требований, но и рассмотрение требований по контролю уровня профессиональных конференций.

Следует отметить, что часть международных стандартов, упомянутых в этой статье, гармонизированы до уровня национальных стандартов РФ. Наличие данной тенденции позволяет надеяться, что после утверждения стандартов ISO/IEC 27021 и ISO/IEC 19896-1 на уровне ИСО в Российской Федерации достаточно быстро появятся их аналоги.

СПИСОК ЛИТЕРАТУРЫ:

1 Tolstoy A., Miloslavskaya N. Professional Competencies Level Assessment for Training of Masters in Information Security. In book: Information Security Education Across the Curriculum. IFIP Advances in Information and Communication Technology. 9th IFIP WG 11.8 World Conference, WISE 9, Hamburg, Germany, May 26-28, 2015, Proceedings. ISBN 978-3-319-18499-9. ISSN 1868-4238. Springer International Publishing. Vol. 453, 2015, pp. 135-145.
2 Bishop, M., Engle, S. The Software Assurance CBK and University Curricula. 10th Colloquium for Information Systems Security Education. University of Maryland, U.S.A (2006). URL: http://nob.cs.ucdavis.edu/bishop/talks/2006-cisse-1/swacbk.pdf (access date 28.10.2015).
3 Fischer-Hübner, S., Yngström, L. (Eds.): WISE 1: Proceedings of the IFIP WG 11.8 First World Conference on Information Security Education, 17-19 June 1999, Kista, Sweden.
4 Armstrong, H., Yngström, L. (Eds.): WISE 2: proceedings of the IFIP WG 11.8 Second World Conference on Information Security Education: 12-14 July 2001, Perth, Australia.
5 Irvine, C.E., Armstrong, H.L. (Eds.): Security Education and Critical Infrastructures, IFIP WG11.8 Third Annual World Conference on Information Security Education (WISE3), June 26-28, 2003, Monterey, California, U.S.A. Kluwer 2003.
6 Miloslavskaya N., Tolstoy A. State-Level Views on Professional Competencies in the Field of IoT and Cloud Information Security. Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Intercloud and IoT (ICI 2016). Vienna (Austria), 22-24 August 2016. Pp. 83-90.
7 State Government Information Security Workforce Development Model. A Best Practice Model and Framework. June 2010. Final Version 1.0 (U.S.).
8 The U.S. National Cybersecurity Workforce Framework. URL: https://www.dhs.gov/ national-cybersecurity-workforce-framework (access date 28.10.2015).
9 The Cyber Security Capability Framework & Mapping of ISM Roles. Final Report. Australian Government Information Management Office. June 2010.
10 The European e-Competence Framework 3.0. A common European Framework for ICT Professionals in all industry sectors. CWA 16234:2014 Part 1. CEN.
11 ISO/IEC 27001:2013 "Information technology -- Security techniques – Information security management systems — Requirements".

REFERENCES:

[1] Tolstoy A., Miloslavskaya N. Professional Competencies Level Assessment for Training of Masters in Information Security. In book: Information Security Education Across the Curriculum. IFIP Advances in Information and Communication Technology. 9th IFIP WG 11.8 World Conference, WISE 9, Hamburg, Germany, May 26-28, 2015, Proceedings. ISBN 978-3-319-18499-9. ISSN 1868-4238. Springer International Publishing. Vol. 453, 2015, pp. 135-145.
[2] Bishop, M., Engle, S. The Software Assurance CBK and University Curricula. 10th Colloquium for Information Systems Security Education. University of Maryland, U.S.A (2006). URL: http://nob.cs.ucdavis.edu/bishop/talks/2006-cisse-1/swacbk.pdf (access date 28.10.2015).
[3] Fischer-Hübner, S., Yngström, L. (Eds.): WISE 1: Proceedings of the IFIP WG 11.8 First World Conference on Information Security Education, 17-19 June 1999, Kista, Sweden.
[4] Armstrong, H., Yngström, L. (Eds.): WISE 2: proceedings of the IFIP WG 11.8 Second World Conference on Information Security Education: 12-14 July 2001, Perth, Australia.
[5] Irvine, C.E., Armstrong, H.L. (Eds.): Security Education and Critical Infrastructures, IFIP WG11.8 Third Annual World Conference on Information Security Education (WISE3), June 26-28, 2003, Monterey, California, U.S.A. Kluwer 2003.
[6] Miloslavskaya N., Tolstoy A. State-Level Views on Professional Competencies in the Field of IoT and Cloud Information Security. Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud

Workshops. The 3rd International Symposium on Intercloud and IoT (ICI 2016). Vienna (Austria), 22-24 August 2016. Pp. 83-90.
[7] State Government Information Security Workforce Development Model. A Best Practice Model and Framework. June 2010. Final Version 1.0 (U.S.).
[8] The U.S. National Cybersecurity Workforce Framework. URL: https://www.dhs.gov/ national-cybersecurity-workforce-framework (access date 28.10.2015).
[9] The Cyber Security Capability Framework & Mapping of ISM Roles. Final Report. Australian Government Information Management Office. June 2010.
[10] The European e-Competence Framework 3.0. A common European Framework for ICT Professionals in all industry sectors. CWA 16234:2014 Part 1. CEN.
[11] ISO/IEC 27001:2013 "Information technology -- Security techniques – Information security management systems — Requirements".

Поступила в редакцию - 21 июля 2017 г. Окончательный вариант – 09 ноября 2017 г.
Received – July 21, 2017. The final version – November 09, 2017.

Николай С. Егошин, Антон А. Конев, Александр А. Шелупанов
Томский государственный университет систем управления и радиоэлектроники,
пр-т. Ленина, д. 40, г. Томск, 634050, Россия,
e-mail: ens@csp.tusur.ru, ORCID 0000-0003-4770-0701,
e-mail: kaa@keva.tusur.ru, ORCID 0000-0002-3222-9956,
e-mail: saa@keva.tusur.ru, ORCID 0000-0003-2393-6701

ФОРМИРОВАНИЕ МОДЕЛИ НАРУШИТЕЛЯ*

DOI: http://dx.doi.org/10.26583/bit.2017.4.02

Аннотация. Под моделью нарушителя понимаются предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности. Модель нарушителя является важной частью информационной безопасности организации. Важно понимать, что игнорирование или недобросовестное построение модели «для галочки» может серьезно отразиться на сохранности конфиденциальной информации и привести к ее потере. Модель нарушителя носит неформальный характер, и, как следствие, не существует строго однозначной методики по составлению таковой. Множество авторов в научно-технической литературе описывает различные методы классификации нарушителей, меж тем многие специалисты по информационной безопасности, работающие на предприятиях, вынуждены составлять свои нормативно-методические документы, так как существующие модели далеко не всегда удовлетворяют всем особенностям работы организации. Несмотря на то, что многие модели имеют высокий уровень корреляции между классификационными признаками, выработать единую модель до сих пор не удалось. В данной работе предпринимается попытка разработки своей собственной методики формирования модели нарушителя. Перед началом работы были сформированы следующие задачи научно-исследовательской работы: 1) изучить существующие методики построения модели нарушителя; 2) выявить недостатки существующих методик; 3) разработать модель нарушителя и методику составления перечня наиболее вероятных нарушителей, учитывающую выявленные недостатки. В ходе работы были проанализированы несколько существующих моделей нарушителя, в результате этого были выявлены их недостатки и определены сложности, на которые было обращено внимание при разработке собственной модели нарушителя. В разработанной модели были построены причинно-следственные связи между элементами модели и цепочками предполагаемых последствий, описаны и ранжированы возможные виды предполагаемых нарушителей. Модель позволяет строить более полное описание нарушителя информационной безопасности.

Ключевые слова: модель нарушителя, модель угрозы, информационная безопасность, конфиденциальная информация.

Для цитирования. **ЕГОШИН, Николай С.; КОНЕВ, Антон А; ШЕЛУПАНОВ, Александр А.** ФОРМИРОВАНИЕ МОДЕЛИ НАРУШИТЕЛЯ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 19-26, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/273>. Дата доступа: 28 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.02.

***Благодарности:** Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУР на 2017-2019 год (проект №2.8172.2017/8.9).

Nikolay S. Egoshin, Anton A. Konev, Alexander A. Shelupanov
Tomsk State University of Control Systems and Radioelectronics,
Lenin Av., 40 Tomsk, 634050, Russia
e-mail: ens@csp.tusur.ru, ORCID 0000-0003-4770-0701
e-mail: kaa@keva.tusur.ru, ORCID 0000-0002-3222-9956
e-mail: saa@keva.tusur.ru, ORCID 0000-0003-2393-6701

Building a model of infringer

DOI: http://dx.doi.org/10.26583/bit.2017.4.02

Abstract. By a model of infringer one means a set of assumptions about the specific (restricted) tools of the infringer, which the latter can use to conduct attacks. The infringer model is an important part of the organization's information security. One should realize that ignoring the model, or building it without due care, can seriously affect the security of confidential information and lead to its loss. The infringer model is informal, which implies the absence of strict and unambiguous methodology for developing such a model. There exist many academic and technical publications proposing various methods of classifying violators. Meanwhile, many information security practitioners are forced to create their own normative and methodological documents, because existing models do not necessarily capture all the aspects of the organization's work. Despite the fact that many models have a high level of correlation between classification characteristics, it has not been possible to work out a unified model so far. We attempt to develop our own methodology for building the infringer model. We have started this project by outlining the roadmap: (1) study the existing methods of constructing the infringer model; (2) identify shortcomings of existing methods; (3) develop a model of the infringer and a methodology for listing the most likely violators, with taking into account the identified shortcomings. In the process of implementation of the plan, we have analyzed several existing models of infringer and revealed their shortcomings and inherent difficulties. In the developed model, causal relationships between the elements of the model and the chains of the alleged consequences have been constructed, and possible types of alleged violators have been described and ranked. As a result, our model allows one to create a more deep description of the infringer.
Keywords: model of infringer, threat model, information security, confidential information

For citation. **EGOSHIN, Nikolay S; KONEV, Anton A; SHELUPANOV, Aleksander A.** Building a model of infringer. IT Security, [S.l.], v. 24, n. 4, p. 19-26, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/273>. Date accessed: 28 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.02.

***Acknowledgements:** The work was executed at financial support of the Ministry of education and science of the Russian Federation within the basic part of state task TUSUR in 2017-2019 year. (project No. 2.8172.2017/8.9).

Преступления, в том числе и компьютерные, совершаются людьми. Пользователи системы и ее персонал, с одной стороны, являются составной частью, необходимым элементом автоматизированных систем (АС). С другой стороны, они же являются основной причиной и движущей силой нарушений и преступлений.

Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Исследовав причины нарушений, можно либо повлиять на сами эти причины (конечно если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлении.

Нарушитель - это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства [1].

Под моделью нарушителя понимаются предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Модель нарушителя является важной частью в обеспечении информационной безопасности организации. Важно понимать, что игнорирование или недобросовестное построение модели «для галочки» может серьезно отразиться на сохранности конфиденциальной информации и привести к ее потере. Исходя из этого, решение

проблемных вопросов формирования модели нарушителя является одним из первоочередных и важных направлений обеспечения информационной безопасности.

Модель нарушителя носит неформальный характер, и, как следствие, не существует строго однозначной методики по составлению таковой. Множество авторов в научно-технической литературе описывает различные методы классификации нарушителей, несмотря на это, некоторые специалисты по информационной безопасности, работающие на предприятиях, вынуждены составлять свои нормативно-методические документы, так как существующие модели далеко не всегда удовлетворяют всем особенностям работы организации. И хотя большинство моделей и имеют высокий уровень корреляции между классификационными признаками, выработать единую модель до сих пор не удалось [2]. А между тем, существование единой универсальной модели имеет очевидное преимущество в виду того, что неполнота описания влечёт за собой необходимость доработки модели под нужды конкретной организации о чём было сказано ранее. Данное действие не всегда может быть корректно осуществлено по различным причинам (будь то недостаточный профессионализм сотрудника, либо банальная нехватка времени). Возможная избыточность модели не нанесёт вреда, в то время как пробелы в описании вероятных нарушителей могут оставить «дыры» в системе безопасности.

В данной работе осуществляется разработка своей собственной методики формирования модели нарушителя. Перед началом работы были сформированы следующие задачи научно-исследовательской работы:

1. изучить существующие методики построения модели нарушителя;
2. выявить недостатки существующих методик;
3. разработать модель нарушителя и методику составления перечня наиболее вероятных нарушителей, учитывающую выявленные недостатки.

В ходе работы были проанализированы несколько существующих моделей нарушителя, а именно: модель нарушителя по требованиям ФСТЭК России [3] и ФСБ России [4], модель нарушителя по требованиям руководящего документа Гостехкомиссии [5], модель угроз и нарушителя Минсвязи [6] и иные неформальные модели нарушителя [7, 8, 9, 10, 11, 12].

В результате анализа упомянутых моделей были выявлены их недостатки и определены сложности, на которые следует обратить внимание при разработке собственной модели нарушителя:

- некоторые модели рассматривают нарушителя исключительно как злоумышленника (например, [7]), мало упоминаний случайных ошибок, действий стихийного характера и природных явлений;
- модели представляют из себя описание примеров действий нарушителя, формулировки нередко многословны и сложны для восприятия;
- отсутствует универсальность разработанных моделей, например, модель [10] нельзя применить к системе, описываемой в работе [12] и наоборот;
- обширное использование лингвистических шкал оценок, что недопустимо для корректной оценки возможностей нарушителя.

Учитывая недостатки описанных ранее моделей можно составить перечень основных параметров нарушителя информационной безопасности, на основе которых будет строиться новая модель описания нарушителя:

Таблица 1 – Параметры нарушителя информационной безопасности

Параметр	Значение
M(otivation) – преднамеренность совершения нарушения	0-случайное, 1-преднамеренное
P(lace) – положение относительно организации, работающей с информацией	0-внешний, 1-внутренний
T(ype) – типнарушителя	4 типа на основе M и P (00, 01, 10, 11)
I(nformation) – знание рубежа защиты и уязвимости в нём	Отсутствие(0)/наличие (1)
E(xtra) – возможность использования несанкционированного средства обработки информации	Отсутствие(0)/наличие (1)
O(ff) – возможность отключения рубежа защиты	Отсутствие(0)/наличие (1)
D(isruption) – возможность нарушения работы рубежа защиты	Отсутствие(0)/наличие (1)
A(ttack) – возможность преодоления рубежа защиты	Отсутствие(0)/наличие (1)
Q(uality) – уровеньнарушителя	От 0 до 7 согласно схеме (рис.1)
Th(reat) – привязка к определенной угрозе	Отсутствие(0)/наличие (1)
N(umber) – количество рубежей защиты, которые осталось преодолеть	0-санкционированный пользователь, (число большее нуля) – несанкционированный

Условно параметры можно разделить на 2 части: а) параметры, описывающие тип (M, P и T) и качества нарушителя (I, E, O, D, A, Q); б) параметры, характеризующие систему защиты (Th и N).

Из схемы (рис. 1) видно, что в формируемой модели нарушителя произведено разделение:

- тип/качество нарушителя;
- поиск и использование уязвимости;
- произведено условное отделение санкционированных и несанкционированных действий и средств.

Для удобства пользователей данной модели нарушителя введена условная бальная система. По мере возрастания опасности от каждого нарушителя относительно каждого возможного действия поставлен определенный балл. Превосходство санкционированных средств над несанкционированными вызвано тем, что нарушитель, использующий санкционированные, то есть разрешенные самой системой, действия является гораздо более опасным, чем нарушитель, которому не хватает навыков и/или которому приходится использовать сторонние средства для достижения своей цели[13].

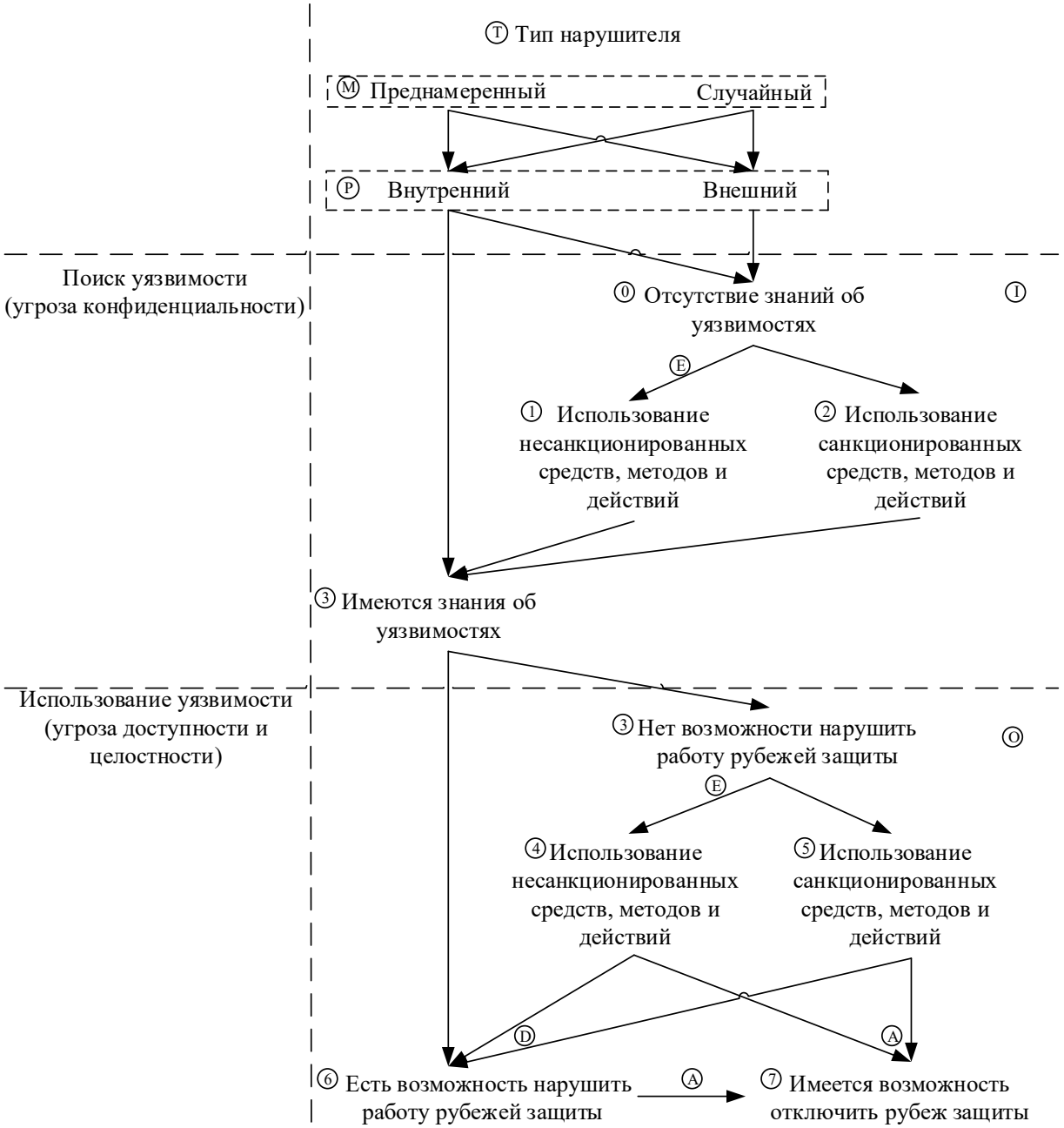


Рисунок 1 – Схема отображения параметров нарушителя
(Fig. 1 – Diagram display options of the offender)

Разделение же уровней нарушителя на поиск и использование уязвимостей вызвано тем, что действия нарушителя носят двойственный характер по отношению к информации о рубежах и к системе, в которой хранится конфиденциальная информация. Владея информацией об уязвимостях в рубежах, нарушитель может лишь рассказать эту информацию кому-либо, что само по себе представляет угрозу конфиденциальности. Имея же информацию об уязвимостях и в попытке ее использовать, нарушитель осуществляет угрозу доступности компонентов рубежа, целостности рубежа и всей системы в целом.

Разделение так же вызвано тем, что при каждом из этих действий нарушитель будет использовать разные средства: в первом случае нарушитель будет искать уязвимости, что больше носит пассивный характер, а во втором уже использовать, что носит уже гораздо более активный характер.

Исходя их этой схемы (рис. 1), можно сделать предположения о том, кем может являться нарушитель для каждого уровня, который на ней изображен:

0 уровень – простой внешний либо внутренний нарушитель с очень ограниченным доступом, (например, уборщица), у которых нет мотивации;

1 уровень – простой внешний либо внутренний нарушитель с очень ограниченным доступом, которые для выявления угроз используют несанкционированные средства для получения информации об уязвимостях в рубежах защиты. Например, следят за тем, что происходит в окнах здания из неконтролируемой территории;

2 уровень – нарушитель, который использует своё положение чтобы собирать информацию об уязвимостях в рубежах защиты, используя санкционированные методы. Например, ходить по зданию и высматривать положение камер наблюдения;

3 уровень – нарушитель, обладающий информацией об уязвимостях, может быть, как сотрудником, имеющим отношение к конструированию данного рубежа защиты, так и одним из нарушителей, ранее имевших 1 или 2 балла, при условии, что их действия не были замечены и пресечены сотрудниками охраны;

4 уровень – изначально внутренний нарушитель, имеющий достаточно информации про уязвимости в рубеже, но не имеющий возможности нарушить или преодолеть защиту рубежа, используя свой уровень допуска и использующий для этого несанкционированные средства. Примером может быть сотрудник, работающий на другом этаже здания с другим видом информации, но знающий общую схему здания, расположение и уязвимости в рубежах защиты. Этот сотрудник мог принести плоскогубцы и с их помощью вывести из строя камеры наблюдения. Перенося эту ситуацию в виртуальную среду можно сделать предположение, что потенциальным нарушителем может являться пользователь внутренней компьютерной сети здания, имеющий пароль для входа в операционную систему, но не имеющий доступа к определенной информации и использующий для этого программы-переборщики паролей;

5 уровень – изначально внутренний нарушитель, который для достижения своих целей использует санкционированные методы. Например, пользователь, имеющий пароль к необходимой информации может пересылать конфиденциальные данные другому санкционированному пользователю, работающему за территорией этого здания, например, в филиале, используя заведомо ненадежный канал передачи данных;

6 уровень – изначально внутренний нарушитель с высоким уровнем доступа, имеющий возможность нарушить работу рубежей защиты, пользуясь своим служебным положением. Таким сотрудником может быть администратор информационной безопасности;

7 уровень – изначально внутренний нарушитель с очень высоким уровнем доступа, имеющий возможность отключить рубеж защиты, используя своё служебное положение.

Таким сотрудником может являться администратор системы защиты либо работник охраны. Так же под это описание подходят форс-мажорные обстоятельства (например, природные катастрофы, так как природе перед стихийными бедствиями не нужно получать информацию о рубежах защиты и отключать их).

Следует также отметить, что привязка нарушителя осуществляется к угрозе, которая влияет непосредственно на информацию, остальные же пункты закреплены за охраняющими эту информацию рубежами защиты, так как при устранении всех рубежей информация автоматически становится доступной и тот, кто нарушил целостность рубежей получает ее в свое распоряжение[14].

Схематически работу предлагаемой методики формирования модели нарушителя с использованием известной из системного анализа модели черного ящика можно представить следующим образом (рис. 2).

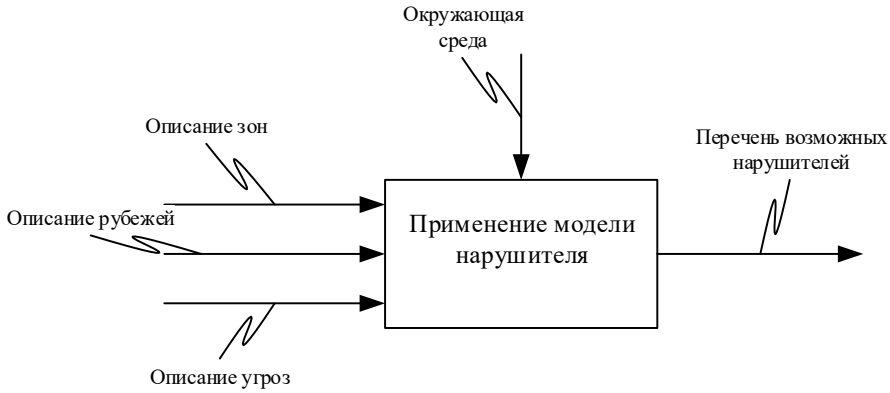


Рисунок 2– Схематическое описание работы модели нарушителя безопасности с использованием черного ящика
(Fig. 2– Schematic description of the operation of the intruder model security using the black box)

В итоге, методика формирования модели нарушителя действует следующим образом:

1. описываются все зоны, окружающие конфиденциальную информацию[15];
2. описываются все рубежи защиты между зонами и внутри них[15];
3. описываются возможные угрозы;
4. описывается состояние окружающей среды;
5. приведенные описания применяется к схеме (рис. 1)в результате чего формируется и получается описание вероятных нарушителей информационной безопасности.

Таким образом, в разработанной модели были построены причинно-следственные связи между элементами модели и цепочками предполагаемых последствий. Основываясь на этом, а также на описании состояния окружающей среды, рубежей защиты и всех зон, окружающих конфиденциальную информацию, были описаны и ранжированы возможные виды предполагаемых нарушителей. Как следствие, модель позволяет построить полное и универсальное по отношению к различным системам описание вероятного нарушителя информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1 Герасименко В. А. Основы защиты информации в автоматизированных системах: В 2 кн. – Кн. 2. – М.: Энергоатомиздат, 1994. – 176 с.

2 Стефаров А. П., Жукова М. Н. О сравнении моделей нарушителя правил разграничения доступа в автоматизированных системах. Информационное противодействие угрозам терроризма. 2013. № 20. С. 147-151.

3 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка): методика, утв. ФСТЭК России 15.02.2008. Собрание законодательства. 2008. 156 с.

4 Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации [Текст] : утв. Руководством 8 Центра ФСБ России 21 февр. 2008 года № 149/54-144. – М., 2008. – 20 с.

5 Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: руководящий документ, утв. РД Гостехкомиссии 30.03.1992.

6 Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли: методика, одобрено секцией №1 Научно-технического совета Минкомсвязи России «Научно-техническое и стратегическое развитие отрасли» от 21.04.2010.

7 Белоножкин В. И. Модель нарушителя безопасности региональной антитеррористической ИАС. Информация и безопасность. 2006. № 2. С. 155-157.

8 Федюнина А. П., Коломина И. В. Неформальная модель нарушителя в информационной сфере. Вестник Астраханского государственного технического университета. 2007. № 3. С. 166-168.
9 Гришина Н. В. Модель потенциального нарушителя объекта информатизации. Известия ЮФУ. Технические науки. 2003. С. 356-358
10 Аютова И. В. Модель нарушителя безопасности ВУЗа. Сборники конференций НИЦ Социосфера. № 8. 2012. С. 372-388.
11 Чебанов А.С., Жук Р.В., Власенко А.В., Сазонов С.Ю. Модель нарушителя комплексной системы обеспечения информационной безопасности объектов защиты. Известия Юго-Западного государственного университета. Серия: управление, вычислительная техника, информатика, медицинское приборостроение. 2013. № 1. С. 171-173.
12 Десницкий В.А., Чеулин А.А. Обобщенная модель нарушителя и верификация информационно-телекоммуникационных систем со встроенными устройствами. Технические науки – от теории к практике. 2014. № 39. С. 7-21.
13 Novokhrestov A., Konev A. Mathematical model of threats to information systems. AIP conference proceedings. 2016. vol. 1772. pp. 060015.
14 Скрыль С. В., Исаев О. В. Имитационное моделирование процесса преодоления «моделью» нарушителя комплексов средств охраны. Вестник Воронежского института ФСИН России. 2013. № 1. С. 65-67.
15 Конев А.А., Давыдова Е.М. Подход к описанию структуры системы защиты информации. Доклады ТУСУР. 2013. №2(28). С. 107–111.

REFERENCES:

[1] Gerasimenko V. A. Basics of information protection in automated systems: In 2 books – Book 2. – M.: Jenergoatomizdat, 1994. – 176 p. (in Russian).
[2] Stefarov A. P., Zhukova M. N. On comparing models of rule-breaker access security in automated systems. Informacionnoe protivodejstvie ugrozam terrorizma. 2013. № 20. P. 147-151. (in Russian).
[3] Bazovaja model' ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh (vypiska): metodika, utv. FSTJeK Russia. 15.02.2008 // Sobranie zakonodatel'stva. 2008. 156 p. (in Russian).
[4] Metodicheskie rekomendacii po obespecheniju s pomoshh'ju kriptosredstv bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh s ispol'zovaniem sredstv avtomatizacii [Tekst] : utv. Rukovodstvom 8 Centra FSB Rossii 21 fevr. 2008 goda № 149/54-144. – M., 2008. – 20 p. (in Russian).
[5] Koncepcija zashhity sredstv vychislitel'noj tehniki i avtomatizirovannyh sistem ot nesankcionirovannogo dostupa k informacii: rukovodjashhij dokument, utv. RD Gostehkomissii 30.03.1992. (in Russian).
[6] Model' ugroz i narushitelja bezopasnosti personal'nyh dannyh, obrabatyvaemyh v tipovyh informacionnyh sistemah personal'nyh dannyh otrasli: metodika, odobreno sekciej №1 Nauchno-tehnicheskogo soveta Minkomsvjazi Rossii «Nauchno-tehnicheskoe i strategicheskoe razvitie otrasli» ot 21.04.2010. (in Russian).
[7] Belonozhkin V. I. Model intruder security regional counter-terrorism IAS. Informacija i bezopasnost'. 2006. № 2. P. 155-157. (in Russian).
[8] Fedjunina A. P., Kolomina I. V. An informal model of the intruder in the field of information. Vestnik Astrahanskogo gosudarstvennogo tehnicheskogo universiteta. 2007. № 3. P. 166-168. (in Russian).
[9] Grishina N. V. Model potential intruder object of Informatization. Izvestija JuFU. Tehnicheskie nauki. 2003. P. 356-358. (in Russian).
[10] Ajutova I. V. Model of the offender security of the University. Sborniki konferencij NIC Sociosfera. № 8. 2012. P. 372-388. (in Russian).
[11] Chebanov A.S., Zhuk R.V., Vlasenko A.V., Sazonov S.Ju. The intruder model complex systems of information security protection. Izvestija Jugo-Zapadnogo gosudarstvennogo universiteta. Serija: upravlenie, vychislitel'naja tehnika, informatika, medicinskoe priborostroenie. 2013. № 1. P. 171-173. (in Russian).
[12] Desnickij V.A., Cheulin A.A. A generalized model of the offender and verification of information and telecommunication systems with embedded devices. Tehnicheskie nauki – ot teorii k praktike. 2014. № 39. P. 7-21. (in Russian).
[13] Novokhrestov A., Konev A. Mathematical model of threats to information systems // AIP conference proceedings. 2016. vol. 1772. pp. 060015.
[14] Skryl' S. V., Isaev O. V. Simulation of the process of overcoming a "model" offender of complexes of means of protection. Vestnik Voronezhskogo instituta FSIN Rossii. 2013. № 1. P. 65-67. (in Russian).
[15] Konev A.A., Davydova E.M. Approach to the description of the structure of information security system. Doklady TUSUR. 2013. №2(28). P. 107–111. (in Russian).

Поступила в редакцию – 03 августа 2017 г. Окончательный вариант – 09 ноября 2017 г.
Received – August 03, 2017. The final version – November 09, 2017.

Виктор С. Горбатов[1], Игорь Ю. Жуков[2], Олег Н. Мурашов[2]
[1]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, г. Москва, 115409, Россия
e-mail: VSGorbatov@mephi.ru, ORCID 0000-0001-9998-9733
[2]ООО «Национальный мобильный портал», Волгоградский пр., 2, офис 36, Москва, 109316, Россия
e-mail: i.zhukov@inbox.ru, ORCID 0000-0002-4429-8799
e-mail: olegxozbox@yandex.ru, ORCID 0000-0002-4467-2170

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ АУТЕНТИФИКАЦИИ И ВЫРАБОТКИ ОБЩЕГО КЛЮЧА КОНТРОЛЬНЫХ УСТРОЙСТВ АВТОТРАНСПОРТА

DOI: http://dx.doi.org/10.26583/bit.2017.4.03

Аннотация. В работе описывается протокол выработки общего ключа с аутентификацией абонентов, предназначенного для использования в бортовых устройствах (тахографах), которые устанавливаются на транспортные средства с целью обеспечения транспортной безопасности дорожного движения. Данный протокол основан на применении известных отечественных криптографических преобразований и направлен на обеспечение целостности и аутентичности данных, передаваемых по каналу связи между бортовым устройством и картами тахографа, входящими в состав контрольных устройств автотранспортных средств. Протокол разработан в соответствии с рекомендациями Росстандарта по принципам разработки и модернизации шифровальных (криптографических) средств защиты информации, оформлен в виде проекта национального стандарта, предлагаемого для общественного обсуждения и утверждения в установленном порядке. Основным результатом данного исследования является формулирование определенных свойств безопасности, идентичных тем задачам, которые ставит перед собой нарушитель с целью его компрометации. Учет методов компрометации позволяет уже на этапе создания протокола заложить в него структурные особенности, обеспечивающие выполнение заданных свойств безопасности и последующее обоснование их достаточности.

Ключевые слова: безопасность транспорта, бортовое устройство, криптографический протокол, механизмы аутентификации, свойства безопасности

Для цитирования. **ГОРБАТОВ, Виктор С; ЖУКОВ, Игорь Ю; МУРАШОВ, Олег Н.** КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ АУТЕНТИФИКАЦИИ И ВЫРАБОТКИ ОБЩЕГО КЛЮЧА КОНТРОЛЬНЫХ УСТРОЙСТВ АВТОТРАНСПОРТА. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 27-34, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/274>. Дата доступа: 28 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.03.

Victor S. Gorbatov[1], Igor Y. Zhukov[2], Oleg N. Murashov[2]
[1]National Research Nuclear University MEPHI
Kashirskoe shosse, 31,Moscow, 115409, Russia
e-mail: VSGorbatov@mephi.ru, ORCID 0000-0001-9998-9733
[2]Ltd «The National Mobile Portal», Volgogradskiy pr., 2 off.36, Moscow, 109316, Russia
e-mail: i.zhukov@inbox.ru, ORCID 0000-0002-4429-8799
e-mail: olegxozbox@yandex.ru, ORCID 0000-0002-4467-2170

Authentication and common key generation cryptographic protocol for vehicle tachographs

DOI: http://dx.doi.org/10.26583/bit.2017.4.03

Abstract. We present a public key generation protocol. The key is used for subscriber authentication in tachographs installed on vehicles in order to provide traffic safety. The protocol is based on the well-known Russian cryptographic algorithms. It ensures integrity and authenticity of data transmitted through communication channel between the on-board devices

and vehicle tachograph cards. The protocol was developed in accordance with the Rosstandart recommendations and complies with the development and modernization principles for data protection encryption (cryptographic) means. The protocol was suggested as a national standard draft and is open for public discussion in accordance with the established procedure.
The main results of our study is the formulation of certain security tasks identical to those used by potential infringers to compromise the protocol. This allows one to account for structural features that will ensure further protocol compliance to the target security characteristics, as well as to guarantee subsequent justification of feature set sufficiency.
Keywords: Smart Building, Management Systems, Internet of Things (IoT)
For citation. **GORBATOV, Victor S.; ZHUKOV, Igor Y.; MURASHOV, Oleg N..** Authentication and common key generation cryptographic protocol for vehicle tachographs. IT Security, [S.l.], v. 24, n. 4, p. 27-34, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/274>. Date accessed: 28 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.03.

1 Взаимная аутентификация

Контрольное устройство автотранспорта – комплект оборудования, предназначенный для обеспечения транспортной безопасности дорожного движения путем перманентной регистрации его основных параметров [1], в частности данных о движении транспортных средств и некоторых периодах работы их водителей. Обычно под контрольным устройством понимается тахограф, как некое бортовое устройство и внешние компоненты [2]: карта тахографа с встроенной микросхемой, предназначенной для проверки идентификационных данных держателя карты (или идентификационные данные соответствующей группы), передачи и хранения данных [1, 2], датчик движения, антенна для приема сигналов глобальных навигационных спутниковых систем и прочее.

Согласно нормативному документу отечественного государственного регулятора в области транспортной безопасности [2] бортовое устройство должно содержать в себе программно-аппаратное шифровальное (криптографическое) средство (блок СКЗИ), реализующее алгоритмы криптографического преобразования информации [2] и обеспечивающее следующие функции: аутентификацию; регистрацию информации в некорректируемом виде в защищенной памяти (защищенный архив блока СКЗИ); хранение конфиденциальной информации, используемой для создания электронной подписи и ее проверки (далее - ключевой информации), а также аутентифицирующей информации.

В основу механизма взаимной аутентификации карты тахографа и бортового устройства положен следующий принцип [1]: каждая сторона должна доказать другой наличие у нее действительной пары ключей, открытый ключ которой сертифицирован общим для участников протокола Удостоверяющим центром. Данный механизм запускается со стороны бортового устройства при вводе карты тахографа в считывающее устройство. Процесс начинается с обмена сертификатами и извлечения открытых ключей и завершается созданием общего сеансового ключа, используемого для обеспечения конфиденциальности передачи информации между картой и бортовым устройством. Процесс обмена информацией, а также проверки сертификатов полностью совпадает с регламентируемой [1] последовательностью шагов.

Протокол взаимной аутентификации и выработки общего ключа инициируется бортовым устройством и представляет собой последовательное выполнение двух команд, направляемых бортовым устройством в карту тахографа, и двух ответов от тахографа в бортовое устройство. Карта тахографа проверяет полученное от бортового устройства сообщение и, если подпись верна, то карта тахографа принимает решение об аутентификации бортового устройства. В противном случае решение об аутентификации бортового устройства не принимается, и протокол завершает свою работу. Бортовое устройство также проверяет полученную от карты тахографа электронную подпись. Если подпись верна, то бортовое устройство принимает решение об аутентификации карты тахографа. В противном случае решение об аутентификации не принимается.

Протокол разработан в соответствии с рекомендациями [3], оформлен в виде проекта национального стандарта [4] и предлагается для общественного обсуждения и дальнейшего утверждения в установленном порядке.

2 Модель нарушителя

С целью обоснования достаточности общепринятых мер криптографической защиты, рекомендуемых для выполнения протокола взаимной аутентификации [3,4] необходимо уточнить модель нарушителя, то есть определить какими возможностями обладает нарушитель и какие задачи ставит перед собой нарушитель, для того чтобы скомпрометировать анализируемый протокол. Традиционно, при анализе криптографических протоколов исследуются возможности нарушителя с использованием модели Долева-Яо [5]. В ней нарушитель может перехватывать все сообщения, передаваемые в ходе протокола, а также производить накопление переданной информации, которая может быть использована для его компрометации. Как известно такой метод компрометации протокола принято называть «пассивным».

Учитывая, что бортовое устройство при общении с картой тахографа использует, как правило, контактный чип, можно допустить, что нарушитель перехватывает всю передаваемую информацию, используя для этого сигналы электромагнитного излучения или специальные технические средства перехвата обмена информацией между участниками протокола. участников. Вопросы противодействия установке на бортовые устройства технических средств перехвата передаваемой информации выходят за рамки настоящего исследования и будут рассмотрены отдельно.

Кроме пассивного перехвата, традиционно, в модели Долева-Яо нарушитель обладает определенными возможностями по модификации, навязыванию, подмене передаваемых сообщений, используя для этого либо накопленную ранее информацию, либо производя вычисления в процессе выполнения протокола. Кроме того, нарушитель может организовывать одновременное выполнение некоторого числа сессий выполняемого протокола. Сессии могут выполняться одновременно как для инициатора протокола (в нашем случае, это бортовое устройство), так и для отвечающей стороны (это карта тахографа). При этом нарушитель может использовать информацию, передаваемую в ходе всех выполняемых сессий протокола. Такой метод компрометации протокола принято называть «активным».

Рассматривая данную модель применительно к исследуемому протоколу, необходимо заметить, что в силу технических особенностей реализации, в каждый период времени бортовое устройство и/или карта тахографа могут находиться в состоянии выполнения только одной сессии протокола. С другой стороны, мы можем считать, что нарушитель может использовать специальное техническое устройство, которое может служить каналом передачи и обработки информации, эмулирующим работу одной карты для нескольких легитимных бортовых устройств, и одновременно, работу бортового устройства для нескольких легитимных карт тахографа. В остальном, мы будем считать, что все возможности модели Долева-Яо для нарушителя доступны.

3 Свойства безопасности протокола

Будем называть задачи, которые ставит перед собой нарушитель, свойствами безопасности, и будем считать, что нарушение этих свойств и приводит к компрометации протокола. Поскольку в настоящее время нет единой общепринятой системы классификации свойств безопасности, далее будем придерживаться классификации, изложенной в книгах [5-7]. В соответствии с ней отобраны следующие свойства безопасности:

1. *Сложность компрометации ключевой системы (keysecurity)*

Трудоемкость определения общего сеансового ключа K, вырабатываемого в ходе выполнения протокола, должна быть достаточно высокой, сравнимой с трудоемкостью компрометации алгоритма шифрования, для которого вырабатывается ключ. В работе [2] было высказано замечание, что указанным свойствам должен удовлетворять произвольный протокол выработки общего ключа в предположении, что для взаимной аутентификации абонентов используются долговременные ключи. В нашем случае в качестве долговременных ключей выступают ключи электронной подписи, обозначаемые в тексте рекомендаций по стандартизации [3] соответственно TC.K и VU.K.

2. Сложность определения долговременных ключей (longtermkeyssecurity)

Трудоемкость определения долговременных ключей электронной подписи TC.SK, VU.SK должна быть настолько высокой, чтобы обеспечивать функционирование тахографа, использующего протокол, в течение достаточно большого интервала времени.

3. Защита от чтения вперед/назад (knownkeysecurity)

Каждая сессия выполнения протокола должна вырабатывать уникальный общий сеансовый ключ K. Ситуация, при которой один или несколько общих ключей, выработанных в разных сеансах выполнения протокола, станут известны нарушителю, не должна приводить к компрометации общих ключей, вырабатываемых в других сеансах.

4. Защита при компрометации долговременных ключей (forwardsecrecy)

Компрометация долговременных ключей – ключей электронной подписи TC.SK, VU.SK не должна приводить к компрометации общих ключей, выработанных ранее.

5. *Подтверждение ключа (keyconfirmation*)

После выработки общего сеансового ключа K каждый из абонентов – бортовое устройство и карта тахографа должны обладать уверенностью в том, что другой абонент обладает тем же общим сеансовым ключом K.

6. Взаимная аутентификация участников протокола (mutualauthenticate)

Каждая сторона должна доказать другой стороне наличие у нее действительного секретного ключа, однозначно связанного с доверенным открытым ключом.

7. Защита от подмены владельца ключа (KCI, keycompromiseimpersonation)

Допустим, что долговременный ключ карты тахографа TC.SK скомпрометирован и известен нарушителю, а сертификат соответствующего открытого ключа TC.PK еще не помещен в список отозванных сертификатов, доступных бортовому устройству. В этом случае нарушитель, очевидно, может выдавать себя за владельца скомпрометированной карты перед бортовым устройством. Вместе с тем, подобная ситуация не должна приводить к тому, чтобы нарушитель мог выдавать себя за бортовое устройство перед законным владельцем скомпрометированной карты. Аналогичное свойство должно выполняться в случае, если нарушителю удастся скомпрометировать долговременный ключ VU.SK бортового устройства.

8. Защита от выработки ключа с третьим участником протокола (unknownkeyshare)

В случае выполнения данного свойства безопасности не должна возникать ситуация при которой бортовое устройство (карта тахографа) считает, что вырабатывает общий секретный ключ с легитимной картой тахографа (бортовым устройством) A, а на самом деле вырабатывает общий секретный ключ с некоторой другой, то же легитимной, картой (бортовым устройством) B.

9. Защита от навязывания ключевых значений (nokeycontrol)

Ни один из участников протокола не может навязать значение общего секретного ключа по своему выбору другому участнику протокола.

Перечисленные свойства безопасности можно условно разделить на две группы: первая накладывает требования к стойкости протокола и невозможности компрометации нарушителем ключевой системы. Вторая группа носит функциональный характер и накладывает требования к аутентификации участников протокола, корректности и качеству выработанного ключа. Таким образом атаки, с помощью которых нарушитель может попытаться нарушить свойства безопасности, можно разделить на два больших класса:

1) пассивные атаки;

2) активные атаки, включая временные атаки, основанные на изучении накопленной информации.

Такое представление помогает в исследовании достаточности мер защиты протокола от компрометации, что и будет использовано в дальнейшем исследовании.

4 О выполнении свойств безопасности

Одним из подходов к анализу протоколов является систематическое исследование практических приемов компрометации и разработка определенного перечня принципов и положений, позволяющих предотвратить известные атаки. Их классификации и методы компрометации протоколов могут быть найдены в различных источниках, например, в работах [5-7]. Учет методов компрометации протоколов позволяет уже на этапе создания протокола заложить в него структурные особенности, обеспечивающие защиту и выполнение изложенных ранее свойств безопасности. Рассмотрим эту возможность для ряда указанных выше свойств безопасности применительно к исследуемому протоколу.

4.1 Защита от чтения вперед/назад

Данное свойство безопасности предъявляется к протоколам для того, чтобы в случае компрометации общего секретного ключа, выработанного в одном из сеансов протокола, обеспечить секретность передаваемой в других сеансах протокола информации. Единственное, что может связывать в исследуемом протоколе общие сеансовые ключи, выработанные в различных сеансах — датчик случайных чисел. Если предположить, что используемый в программно-аппаратной реализации протокола датчик случайных чисел вырабатывает псевдослучайные последовательности, статистически неотличимые от равновероятных, то можно утверждать, что вырабатываемые абонентами точки TC.P и VU.P также равновероятны. В этом случае общие ключи, вырабатываемые в различных сеансах протокола, также могут рассматриваться как независимые случайные величины, равномерно распределенные в V256. Поэтому невозможно построить методы определения общих секретных ключей, отличные от случайного угадывания и можно считать, что для исследуемого протокола выполняется третье свойство безопасности.

4.2 Независимость общего ключа от долговременных ключей абонентов

Долговременными ключами протокола являются ключи электронной подписи абонентов. Поскольку информация об этих ключах никак не используется при генерации общего секретного ключа, можно считать, что для исследуемого протокола выполнено четвертое свойство безопасности.

4.3 Подтверждение ключа

Предложенный протокол обеспечивает явное подтверждение ключа, так как после его завершения каждая из сторон VU и TC удостоверяется в том, что другая сторона

успешно выработала общий ключ. Вероятность ложного подтверждения ключа не превосходит вероятности подбора верного шифртекста для заданного открытого текста при неизвестном ключе и синхропосылке, то есть не превосходит 2-64. Следовательно, можно считать, что для исследуемого протокола выполнено и пятое свойство безопасности.

4.4 Противодействие KCI-атаке

Под KCI-атакой (имперсонификация при компрометации долговременного секретного ключа) понимается [7] атака, при выполнении которой противник, получивший доступ к долговременному секретному ключу абонента A, может выдать себя перед A за любого другого абонента. Если протокол противостоит KCI-атаке, то для него выполнено седьмое свойство безопасности из перечисленного выше перечня свойств. В исследуемом протоколе, при условии стойкости схемы электронной подписи ГОСТ Р 34.10-2012 доступ противника к долговременному секретному ключу TC.SK не даст ему возможности подделать цифровую подпись S1 на шаге 3 протокола, поскольку та зависит от секретного ключа VU.SK. Одновременно, доступ к долговременному секретному ключу VU.SK не даст ему возможности подделать цифровую подпись S2 на шаге 4 протокола, зависящую от секретного ключа TC.SK. Исключением является случай совпадения двух секретных ключей, VU.SK = TC.SK. Если противник пытается выдать себя перед абонентом за него самого (т.е., например, перед VU за VU), то по определению KCI-атаки он имеет доступ к секретному ключу VU.SK и может полностью имитировать его действия, но этот случай является «вырожденным». В противном случае вероятность совпадения двух случайно выбранных секретных ключей можно оценить величиной 1/q.

4.5 Противодействие UKS-атаке

Под UKS-атакой понимается [8] инцидент, в результате которого абоненты вырабатывают общий ключ, но один из них считает его общим с третьим абонентом. При этом компрометации общего ключа как таковой не происходит, но нарушаются требования, связанные с аутентификацией абонентов. Если протокол противостоит UKS-атаке, то для него выполнено восьмое свойство безопасности. Для противодействия указанному виду инцидентов в протоколе следует использовать функцию выработки производного ключа, зависящего от идентификаторов абонентов. Таким образом, в поток сообщений исследуемого протокола включена функция, связывающая сеанс с идентификаторами конкретных абонентов. Для реализации UKS-атак может быть использовано свойство DSKS – Duplicate Signature Key Selection, которым обладают многие схемы цифровой подписи [9], в том числе и ГОСТ Р 34.10-2012. Указанное свойство состоит в возможности для заданного сообщения M и подписи (r, s) подобрать параметры схемы подписи, в данном случае точку эллиптической кривой P` порядка q, а также секретный ключ SK` такие, что подпись (r, s) будет признана корректной подписью, выработанной при помощи ключа SK`, но с отличными параметрами схемы. Для противодействия UKS-атакам, основанным на данном свойстве схемы цифровой подписи ГОСТ Р 34.10-2012, в поток сообщений исследуемого протокола включено вычисление подписей от строк, содержащих в качестве подстроки E1, E2, вычислить которые без знания общего ключа возможно лишь с пренебрежимо малой вероятностью. Таким образом, без знания общего ключа противник не имеет доступа к сообщениям, под которыми ему необходимо подделать подписи для успешной аутентификации. По нашему мнению, для повышения уровня защищенности анализируемого протокола необходимо использовать эллиптические кривые, либо соответствующие рекомендациям по стандартизации Р 50.114-2016, либо получившие положительное заключение государственного регулятора по результатам их криптографических исследований.

4.6 Защита от навязывания

Данное свойство безопасности позволяет каждому из участников протокола быть уверенным в том, что второй участник протокола не навязал ему ключ, выработанный заранее. В генерации общего секретного ключа принимает участие величина $\pi(Q)$, где Q общая для абонентов секретная точка эллиптической кривой. Значения координат этой точки существенным образом зависят от двух случайных значений, вырабатываемых независимо двумя участниками в ходе выполнения протокола. Это не позволяет кому-либо из участников протокола навязать другому значение точки Q, а, следовательно, и общего секретного ключа. Следовательно, мы можно считать, что для исследуемого протокола выполнено девятое свойство безопасности.

Заключение

Таким образом, в исследуемом криптографическом протоколе аутентификации и выработки общего ключа контрольных устройств автотранспорта уже заложены структурные свойства, позволяющие обеспечить выполнение ряда свойств безопасности и предусмотреть методы защиты от большого класса известных атак. Следующим этапом исследования должно стать полное обоснование достаточности мер противодействия известным атакам и методам компрометации исследуемого протокола с целью рекомендации для его практического применения.

СПИСОК ЛИТЕРАТУРЫ:

1 Европейское соглашение по работе экипажей транспортных средств, производящих международные автомобильные перевозки (ЕСТР). Европейская экономическая комиссия. Комитет по внутреннему транспорту. Записка секретариата. Добавление 1B к приложению ЕСТР, содержащее требования к конструкции, испытаниям, установке и инспекции цифрового контрольного устройства, используемого на автомобильном транспорте. – ECE/TRANS/SC.1/2006/2/Add.1. – 2008.
2 Приказ Минтранса России от 13 февраля 2013г. №36. Эл. Ресурсhttp://www.mintrans.nso.ru/sites/mintrans.nso.ru/wodby_files/files/wiki/2014/12/prikaz_36_13.pdf. Дата обращения 06.06.2017.
3 Росстандарт. Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. — 2016. — 36 стр.
4 Росстандарт. Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Криптографические механизмы аутентификации для применения в контрольных устройствах, обеспечивающих работу автотранспорта (Проект второй редакции). — 2017. — 21 стр.
5 Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. — М.:Академия. — 2009. — 272 с.
6 Boyd C., Mathuria A. Protocols For Authentication And Key Establishment: Springer. — 2003. _ 323 p.
7 Нестеренко А.Ю. Новый протокол выработки общего ключа. Системы высокой доступности. — № 2. — 2012. — стр. 81-90.
8 Diffie W., van Oorschot P., Wiener M. Authentication And Authenticated Key Exchanges. Designs. — 1992. — 2. — P. 107–125.
9 BaekJ., KimK. Remarks. On The Unknown Key-Share Attacks//IEICE Trans. — 2000. — E83-A. — № 12. – P. 99-106.

REFERENCES:

[1] European agreement on work of crews of vehicles engaged in international road transport (AETR). Economic Commission for Europe. The inland transport Committee. Note by the Secretariat. Appendix 1B to the Annex to the AETR related to requirements for construction, testing, installation, and inspection of the digital control device used in road transport.. – ECE/TRANS/SC.1/2006/2/Add.1. – 2008.
[2] Prikaz Mintransa Rossii ot 13 fevralya 2013 g. № 36. EHl. resurs http://www.mintrans.nso.ru/sites/mintrans.nso.ru/wodby_files/files/wiki/2014/12/prikaz_36_13.pdf. Data obrashcheniya 06.06.2017.(In Russian).
[3] Rosstandart. Informacionnaya tekhnologiya. Kriptograficheskaya zashchita informacii. Rekomendacii po standartizacii. Principy razrabotki i modernizacii shifroval'nyh (kriptograficheskih) sredstv zashchity informacii. — 2016. — 36 p. (In Russian).

[4] Rosstandart. Informacionnaya tekhnologiya. Kriptograficheskaya zashchita informacii. Rekomendacii po standartizacii. Kriptograficheskie mekhanizmy autentifikacii dlya primeneniya v kontrol'nyh ustrojstvah, obespechivayushchih rabotu avtotransporta (Proekt vtoroj redakcii). — 2017. — 21 p. (In Russian).
[5] CHeremushkin A.V. Cryptographic protocols. The main characteristics and vulnerabilities.. — M.:Akademiya. — 2009. — 272 p. (In Russian).
[6] Boyd C., Mathuria A. Protocols For Authentication And Key Establishment: Springer. — 2003. – 323 p.
[7] Nesterenko A.YU. The new Protocol develop common key. Sistemy vysokoj dostupnosti. — № 2. — 2012. — P. 81-90. (In Russian).
[8] Diffie W., van Oorschot P., Wiener M. Authentication And Authenticated Key Exchanges. Designs. — 1992. — 2. — P. 107–125.
[9] BaekJ., KimK. Remarks. On The Unknown Key-Share Attacks. IEICE Trans. — 2000. — E83-A. — № 12. – P. 99-106.

Поступила в редакцию - 22 июня 2017 г. Окончательный вариант – 04 ноября 2017 г.
Received – June 22, 2017. The final version – November 04, 2017.

Сергей В. Запечников, Полина О. Кожухова
Национальный исследовательский ядерный университет «МИФИ», Каширское шоссе, 31,г. Москва, 115409, Россия
e-mail: SVZapechnikov@mephi.ru, ORCID 0000-0002-7975-6040
e-mail: PKozhukhova@yandex.ru, ORCID 0000-0002-4004-5209

О КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ СКВОЗНЫХ ЗАЩИЩЕННЫХ СОЕДИНЕНИЙ В МЕССЕНДЖЕРАХ WHATSAPP И TELEGRAM

DOI: http://dx.doi.org/10.26583/bit.2017.4.04

Ключевые слова: криптография, сквозное соединение, шифрование, WhatsApp, Telegram

Аннотация. В статье анализируются возможности повышения стойкости защищенных соединений между пользователями мессенджеров в условиях воздействия внешнего нарушителя и недоверия к провайдеру сервиса. В работе проведено сравнение методов и механизмов криптографической защиты информации, заложенных в основу двух широко распространенных мессенджеров: Telegram и WhatsApp. При этом установлено, что для защиты сквозных соединений в мессенджере Telegram используется протокол MTProto, а в мессенджере WhatsApp — протокол Signal.Изучены особенности реализации мессенджеров на наиболее распространенной мобильной платформе Android, связанные с генерацией случайных чисел. В результате детального анализа каждого из них было выявлено, что лучшим по совокупности свойств безопасности является Signal. Помимо WhatsApp, он используется в ряде других популярных мессенджерах, таких как TextSecure, RedPhone, GoogleAllo, FacebookMessenger, Signal. Выявлены и проанализированы возможные атаки на оба мессенджера. В частности, установлено, что в обоих мессенджерах не защищаются метаданные. Обеспечение безопасности метаданных может стать одной из целей дальнейших исследований.

Для цитирования. **ЗАПЕЧНИКОВ, Сергей В.; КОЖУХОВА, Полина О.** О КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ СКВОЗНЫХ ЗАЩИЩЕННЫХ СОЕДИНЕНИЙ В МЕССЕНДЖЕРАХ WHATSAPP И TELEGRAM. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 35-43, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/275>. Дата доступа: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.04.

Sergey V. Zapechnikov, Polina O. Kozhukhova
National Research Nuclear University MEPhI, Kashirskoe shosse, Moscow, 31, 114509, Russian Federation
e-mail: SVZapechnikov@mephi.ru, ORCID 0000-0002-7975-6040
e-mail: PKozhukhova@yandex.ru, ORCID 0000-0002-4004-5209

On cryptographic security of end-to-end encrypted connections in WhatsApp and Telegram messengers

DOI: http://dx.doi.org/10.26583/bit.2017.4.04

Keywords: cryptography, end-to-end connection, encryption, WhatsApp, Telegram

Abstract. The aim of this work is to analyze the available possibilities for improving secure messaging with end-to-end connections under conditions of external violator actions and distrusted service provider. We made a comparative analysis of cryptographic security mechanisms for two widely used messengers: Telegram and WhatsApp. It was found that Telegram is based on MTProto protocol, while WhatsApp is based on the alternative Signal protocol. We examine the specific features of messengers implementation associated with random number generation on the most popular Android mobile platform. It was shown that Signal has better security properties. It is used in several other popular messengers such as TextSecure, RedPhone, GoogleAllo, FacebookMessenger, Signal along with WhatsApp. A number of possible attacks on both messengers were analyzed in details. In particular, we

demonstrate that the metadata are poorly protected in both messengers. Metadata security may be one of the goals for further studies.

For citation. **ZAPECHNIKOV, Sergey V.; KOZHUKHOVA, Polina O.** On cryptographic security of end-to-end encrypted connections in WhatsApp and Telegram messengers. IT Security, [S.l.], v. 24, n. 4, p. 35-43, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/275>. Date accessed: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.04.

Введение

Одним из самых популярных средств персонального обмена информацией в современном обществе становятся мессенджеры – программы для мгновенного обмена сообщениями и файлами с мобильных устройств и настольных компьютеров. Создатели мессенджеров борются за право называть свои продукты самыми защищенными.

Важным аспектом защиты передаваемых с использованием мессенджеров данных является способ шифрования и аутентификации этих данных. Наилучшим на сегодняшний день считается сквозное защищенное соединение, когда исходящее сообщение обрабатывается на мобильном устройстве отправителя, а обработка входящего сообщения также целиком происходит на мобильном устройстве получателя. Оно используется в таких популярных мессенджерах как WhatsApp и Telegram. Общей чертой такого способа обмена сообщениями в мессенджерах является использование сервера только в роли «почтового ящика». Сервер не получает доступа к содержанию пересылаемых им сообщений. Далее в статье будут рассматриваться только такие способы пересылки сообщений.

Большая распространенность персональных средств интерактивного обмена текстовой информацией и файлами в настоящее время сочетается с недостаточной защищенностью используемых этими программными средствами соединений между участниками диалога, что определяет актуальность исследования этой темы.

1 Обмен сообщениями в Telegram

Telegram — бесплатный кроссплатформенный мессенджер для смартфонов и других устройств, позволяющий обмениваться текстовыми сообщениями и медиафайлами различных форматов [1]. По данным на февраль 2016 года количество активных пользователей в месяц у мессенджера Telegram превысило 100 млн [2].

Для безопасной передачи сообщений между собеседниками в Telegram разработчиками предусмотрен специальный тип соединений — секретные чаты, которые обеспечивают сквозное шифрование и аутентификацию сообщений. Секретные чаты предназначены для общения только двух собеседников, в групповых чатах сквозное шифрование не используется. Для передачи сообщений через секретный чат мессенджер Telegram использует собственный протокол MTProto. Анализ протокола и отдельных элементов его реализации в мессенджере Telegram проводился по материалам [3, 4].

В Telegram обмен сообщениями состоит из трех этапов.

1. *Регистрация клиента*. Клиент вводит свой номер телефона, на который по SMS приходит пятизначный код для подтверждения номера. После этого клиент авторизуется на сервере.

2. *Обмен ключами*. На данном этапе Клиенты вырабатывают общий секретный ключ путем обмена параметрами по протоколу Диффи-Хеллмана.

3. *Обработка исходящего сообщения*. Схема обработки сообщений отправителем представлена на рис. 1.

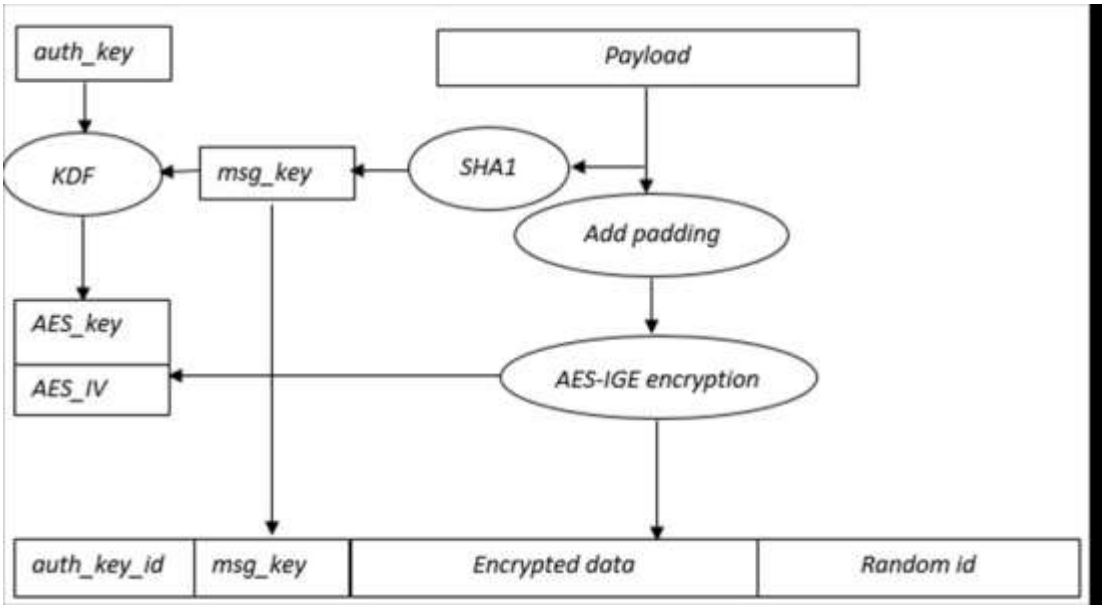


Рисунок 1 - Шифрование сообщений в секретных чатах Telegram
(Fig. 1 - Encryption of messages in a secret chat Telegram)

На рис. 1 приняты следующие обозначения:

-*auth_key*: 2048-битный общий секретный ключ;

-*msg_key*: последние 128 бит SHA1 от сообщения, которое будет зашифровано;

-*padding*: дополнение. 0-96 случайных бит, сгенерированных клиентом, которые добавляются к каждому блоку AES до размера 128 бит;

-*AES key and IV*: 256-битный ключ и 256-битный вектор инициализации, полученные с помощью AES в режиме IGE;

-*auth_key_id*: 64 последних бита SHA1 от auth_key;

-*payload*: заполнение. Заполнение состоит из следующих частей:

• *length*: 32-битное целое число, характеризующее длину Payload (за исключением Length и Padding);

•*header*: 32-битное число, связанное с версией протокола и указанием типа передаваемых медиа-сообщений;

•*random bits*: 128 случайных бит, сгенерированных клиентом, использующихся как соль сообщения;

•*layer*: 32-битное целое число, которое передает информацию о версии протокола клиента;

•*seq_in*: 32-битный счетчик сообщений, отправленных клиентом;

•*seq_out*: 32-битный счетчик сообщений, принятых клиентом;

•*random id*: 64-битное случайное число, сгенерированное клиентом;

•*ttl*: 32-битное целое число, содержащее информацию о количестве секунд, в течение которых принимающий пользователь может увидеть сообщение до того, как оно будет удалено;

•*Padding*: Дополнение. Добавляется перед шифрованием.

-*Message:* отправляемое сообщение.

Новый общий секретный ключ по умолчанию генерируется после отправки каждых очередных ста сообщений.

4. *Обработка входящего сообщения* происходит аналогично этапу 3, но в обратном порядке.

2 Обмен сообщениями в WhatsApp

WhatsApp – бесплатный кроссплатформенный мессенджер с поддержкой голосовой связи. Он позволяет пересылать текстовые сообщения, изображения, видео- и аудиоданные через Интернет. По данным[5], в феврале 2016 г. оценочное число активных пользователей мессенджера WhatsApp превысило миллиард человек и продолжает возрастать.

С апреля 2016 г. в WhatsApp используется сквозное шифрование соединений между пользователями.Сквозное соединение в WhatsApp устанавливается на базе протокола Signal, хотя некоторые точные детали спецификации разработчиками до сих пор не объявлены. В связи с этим анализ протокола и отдельных элементов его реализации в мессенджере WhatsApp проводился по материалам [6 – 8].

В WhatsApp порядок взаимодействия клиентов таков.

1. *Регистрация клиента*. В момент установки мессенджера Клиент генерирует ряд криптографических ключей и регистрируется на Сервере.

2. *Установление сессии*. Клиент, устанавливающий сессию запрашивает с сервера открытые ключи собеседника и оба клиента вырабатывают общие секретные ключи.

3. *Отправка сообщения*. На данном этапе происходит шифрование сообщения ключами, полученными на этапе 2 общими секретными ключами с помощью AES256 в режиме сцепления блоков (CBC).

4. *Обновление «храповика»*. В мессенджере используется специальная криптографическая конструкция – так называемый храповой механизм (ratchet). Он подразумевает обновление ключей собеседников после каждого отправленного и принятого сообщения. На рис. 2 показано, как происходит обновление ключей у клиента при отправке и приеме сообщений. Старые ключи после использования удаляются.

На рис. 3 приняты следующие обозначения:

- *PubK* – открытый ключ;
- *PrK* – секретный ключ;
- *PB1* – открытый ключ клиента B;
- *A1, B*1 – секретные ключи клиентов A и B для шифрования сообщения;
- *RK* – корневой ключ;
- *CH* – ключ цепи.

HKDF определяется следующим образом [9]:

$$\mathrm{HKDF}(XTS, SKM, CTXinfo, L) = K(1)\|K(2)\|...\|K(t), \quad (1),$$

где:

L — число ключевых битов, получаемых в результате применения функции.

K(i) вычисляется по алгоритму, пошагово описанному ниже.

Шаг 1. Вычисляется значение PRK:

$$PRK = \mathrm{HMAC}(XTS, SKM), \quad (2),$$

где:

XTS — случайное заполнение, называемое «солью» (salt), SKM — ключ исходного текста.

Шаг 2. Вычисляется значение K(1):

$$K(1) = \mathrm{HMAC}(PRK, CTXinfo\|0), \quad (3),$$

где:

CTXinfo — ключевая информация (например, идентификаторы алгоритмов, сеансов).

Шаг 3. Вычисляются значения $K(i+1)$:

$$K(i+1) = \mathrm{HMAC}\left(PRK, K(i) \| CTXinfo \| i\right),\ 1 \le i < t\,. \quad (4)$$

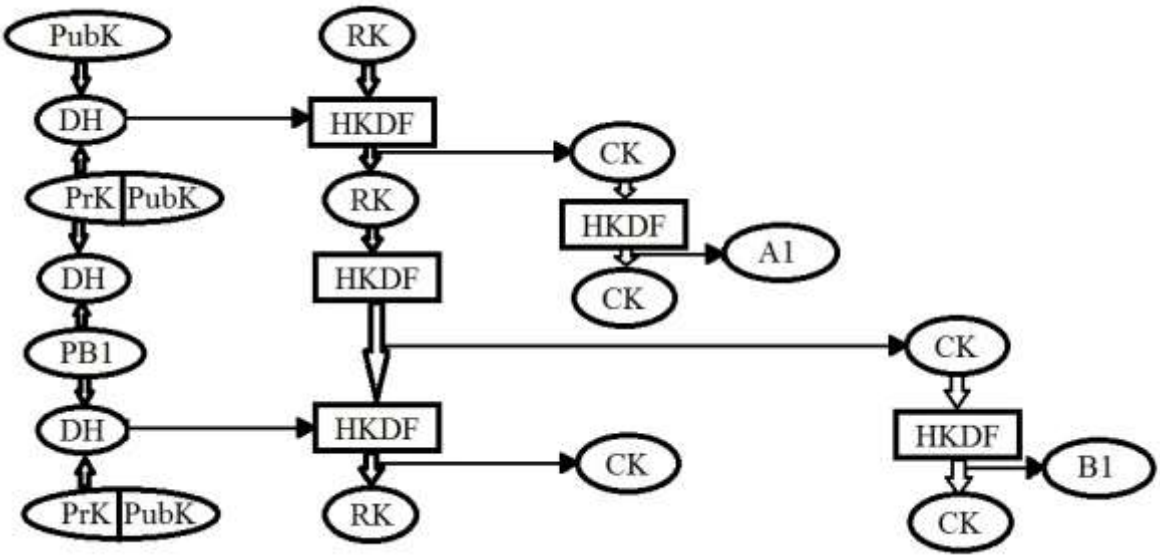


Рисунок 2 - Обновление храповика при отправке и приеме сообщения
(Fig. 2 - Update of the ratchet when sending and receiving messages)

5. *Получение сообщения*. Осуществляется аналогично этапу 3, но в режиме расшифрования.

3 Генерация случайных чисел в устройствах на платформе Android

Мессенджеры используются главным образом на мобильных устройствах. Стойкость используемых в мобильных устройствах криптографических механизмов напрямую зависит от качества генерации случайных величин их операционными системами (ОС). В ходе работы проанализировано устройство генератора случайных величин (ГСЧ) в ОС Android [10]. Выявлено, что он имеет два интерфейса:

- */dev/random* (блокирующий) — возвращает только максимальное число случайных битов, которые содержатся в пуле энтропии. Если в пуле не хватает случайности, то он будет блокировать процесс до того момента, пока счетчик энтропии не накопит достаточное значение;
- */dev/urandom* (неблокирующий) — у данного устройства нет ограничений: будет возвращаться столько битов, сколько запрашивается. Если случайности недостаточно, то поток случайных чисел все равно не прекратится, просто последующие числа будут менее криптостойкими.

В большинстве случаев в качестве случайных чисел берутся значения из неблокирующего пула, что может привести к недостаточному количеству энтропии, и, следовательно, к снижению качества сгенерированных случайных чисел.

Реализация протокола Диффи – Хеллмана на основе эллиптических кривых обладает тем преимуществом, что требуются более короткие ключи, а, следовательно, меньшая зависимость от качества ГСЧ, не способных за короткое время сгенерировать длинную случайную последовательность.

Подробных сведений об устройстве ГСЧ в другой наиболее часто используемой ОС iOS в настоящее время не опубликовано, поэтому судить о качестве этого ГСЧ не представляется возможным.

4 Достоинства и недостатки секретных чатов Telegram

В результате детального анализа алгоритма обработки сообщений в секретных чатах Telegram были выявлены следующие основные достоинства:

- обеспечение защиты от чтения назад, то есть при компрометации будущих ключей предыдущие ключи скомпрометированы не будут;
- обеспечение защиты от чтения вперед, то есть при компрометации предыдущих ключей будущие ключи скомпрометированы не будут;
- возможность устанавливать время жизни отправляемых сообщений.

В то же время следует отметить ряд недостатков принятого в секретных чатах Telegram способа обработки сообщений:

- авторизация по отправке СМС на номер телефона. Недостаток связан с уязвимостью сети SS7. Можно получить доступ к чатам Telegram, секретные чаты прочесть невозможно, зато можно инициировать любой чат от имени жертвы;
- «кустарность» протокола. Разработчики нарушили известный в криптографии принцип – не изобретать самостоятельно новых протоколов, если уже есть протоколы с доказанными оценками стойкости, решающие те же задачи;
- использование обычного «числового» протокола Диффи-Хеллмана. Протокол Диффи-Хеллмана на эллиптических кривых было бы предпочтительнее, так как для него достаточно более коротких случайных чисел. Это позволило бы снизить зависимость стойкости протокола от проблемы качества генерации случайных чисел, описанной в п. 3;
- способ генерации случайных величин существенно зависит от качества ГСЧ в ОС мобильного устройства;
- не обеспечивается безопасность метаданных. Недостаток является существенным, так как на Сервере можно отследить факт передачи сообщений. В дополнение к этому, любой пользователь может добавить к себе в адресную книгу любой номер телефона, который является Клиентом Telegram, и будет знать, когда этот Клиент находится в сети.

5 Достоинства и недостатки чатов WhatsApp

Анализ способа обработки сообщений в WhatsApp позволил выявить следующие его достоинства:

- обеспечение защиты ключей от чтения назад;
- обеспечение защиты ключей от чтения вперед;
- смена ключей после каждого сообщения;
- выработка общего секретного ключа с помощью протокола Диффи-Хеллмана на эллиптических кривых;
- использование протокола с доказанной оценкой стойкости.

В то же время можно заключить, что этому способу присущи следующие недостатки:

- отправка СМС на номер телефона, используемая для аутентификации, является недоверенным способом связи;
- синхронизация с ПК осуществляется через QR-код: такой прием дает множество возможностей для фишинговых атак (пример см. в п. 6);
-способ генерации случайных величин существенно зависит от качества ГСЧ в ОС мобильного устройства;
- не обеспечивается безопасность метаданных о пересылаемых сообщениях.

6 Возможные атаки на клиентов WhatsApp и Telegram

Несмотря на достаточно высокую стойкость протоколов, используемых в мессенджерах Telegram и WhatsApp, остается возможность осуществления целого ряда атак на эти протоколы.

UKS-атака в WhatsApp. Атака описана на основе материалов статьи [8].

A доверяет B, делится ключом. При этом A по факту делится ключом с E.

E — объект нападения, так как A думает, что пишет B, а на самом деле пишет E.

Схема атаки пошагово описана ниже.

Шаг 1. B запрашивает $eprepk_E$ с Сервера.

Шаг 2. B отправляет $eprepk_E$ и ipk_E на Сервер.

Шаг 3. Когда A хочет отправить сообщение B, A запрашивает $prepk_B$, Сервер возвращает $prepk_B$ и ipk_E.

Шаг 4. A вычисляет общий секрет, цепной и корневой ключи.

Шаг 5. A шифрует сообщение и отправляет B.

Шаг 6. B отправляет это сообщение E.

Шаг 7. E расшифровывает сообщение.

Данный вид атаки на сегодняшний момент можно предотвратить только сверкой хэш-кодов ключей.

Атака QRLJacking. Связана с возможностью синхронизации приложения WhatsApp с ПК. При сканировании из WhatsApp QR-кода с ПК все данные синхронизируются. Описание атаки основано на материалах [11].

Схема атаки пошагово описана ниже.

Шаг 1. Злоумышленник инициирует клиентскую QR-сессию и копирует код QR-логина на фишинговую страницу.

Шаг 2. Ссылка на страницу отправляется жертве.

Шаг 3. Жертва сканирует QR-код.

Шаг 4. Происходит процесс аутентификации.

Шаг 5. Злоумышленник получает доступ к аккаунту жертвы.

Атака IND-CCA: Неразличимость шифртекста. Свойство неразличимости шифртекста определяется тем, что противник не должен определить выбранное собеседником сообщение с вероятностью значительно большей, чем 1/2. Если противник может добиться успеха в различении выбранного шифртекста с вероятностью значительно большей, чем 1/2, то считается, что он имеет «преимущество» в различении шифртекста, а схема не считается безопасной с точки зрения неразличимости. Описание атаки основано на материалах исследовании [4].

A будет знать, какое из сообщений зашифровано. Свойство неразличимости не выполняется.

Схема атаки пошагово описана ниже.

Шаг 1. A отправляет B два различных сообщения m0 и m1 одинаковой длины.

Шаг 2. B случайным образом выбирает b = {0, 1} и шифрует сообщение $c = \mathrm{Enc}_{\mathrm{k}}(m_b)$, отправляет его A.

Шаг 3. A добавляет «лишний» блок 128 случайных битов c_r к c: $c' = c \| c_r$ и просит B расшифровать *c'*.

Шаг 4. B расшифровывает *c'* и считывает заполнение *payload*. Все, что идет ниже заполнения *payload*, в том числе и дополнение *padding*, отбрасывается (включая «лишний» блок). B передает $m' = \mathrm{Dec}_{\mathrm{k}}(c') = m_b$.

Шаг 5. A возвращает 1, если $m' = m_1$ и 0, если $m' = m_0$.

Так как длина дополнения *padding* в алгоритме расшифровки не проверяется, то в эту часть передаваемых сообщений можно добавить “лишние” блоки.

Атака, использующая уязвимость «принудительной» смены ключей в WhatsApp. В чатах WhatsApp в случае, когда получатель зашифрованного сообщения долгое время находится в статусе «не в сети» или сменил устройство, генерируется новый ключ. Сообщение пересылается на сервер WhatsApp, где будет ждать появления получателя в сети. То есть появляется посредник с еще одним ключом шифрования, к которому могут получить доступ разработчики. По утверждению [12], администрация мессенджера WhatsApp таким образом может предоставлять сообщения третьим лицам.

Заключение

Таким образом, основные результаты работы заключаются в следующем:

-проанализированы механизмы обеспечения безопасности сквозных защищенных соединений в мессенджерах WhatsApp и Telegram;

-проанализированы способы генерации случайных величин в устройствах на Android;

-выявлены достоинства, недостатки и вероятные атаки в Telegram и WhatsApp.

Результаты работы являются значимыми как в практическом, так и в научном плане, поскольку могут быть использованы для дальнейшего исследования защищенных соединений в мессенджерах с целью усовершенствования алгоритмов передачи информации между клиентами мессенджеров.

СПИСОКЛИТЕРАТУРЫ:

1 Telegram [Электронный ресурс]. URL: https://planfix.ru/docs/Telegram (Дата обращения: 13.11.2016).
2 Число пользователей Telegram превысило 100 миллионов [Электронный ресурс]. URL: https://lenta.ru/news/2016/02/23/telegram/ (Датаобращения: 13.11.2016).
3 Secretchats, end-to-endencryption [Электронныйресурс]. URL: https://core.telegram.org/api/end-to-end(Дата обращения: 13.11.2016).
4 Jacobsen, J. B. A practical cryptanalysis of the Telegram messaging protocol. Ph.D. Theses [Электронныйресурс] / J. B. Jacobsen; Aarhus University: Department of Computer Science. 2015. 79 pp. URL: https://cs.au.dk/~jakjak/master-thesis.pdf (Дата обращения: 20.02.2017).
5 Официальный сайт мессенджера WhatsApp [Электронный ресурс]. URL: https://https://www.whatsapp.com/ (Дата обращения: 27.09.2017).
6 WhatsAppEncryptionOverview [Электронныйресурс]. URL: https://www.whatsapp.com/security/WhatsApp-SecurityWhitepaper.pdf (Дата обращения: 30.11.2016).
7 Cohn-Gordon, K. A Formal Security Analysis of the Signal Messaging Protocol [Электронныйресурс] / K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, D. Stebila. 2016. 30 pp. URL: https://eprint.iacr.org/2016/1013.pdf (Датаобращения: 20.02.2017)
8 Frosch, T. How secure is TextSecure? [Электронныйресурс] / T. Frosch, C. Mainka, C. Bader, F. Bergsma, J. Schwenk, T. Holz. 2014.17 p. URL: https://eprint.iacr.org/2014/904.pdf (Датаобращения: 20.02.2017)
9 Krawczyk, H. Cryptographic Extraction and Key Derivation: The HKDF Scheme [Электронныйресурс] / H. Krawczyk. 2010. 34 pp. URL: https://eprint.iacr.org/2010/264.pdf (Датаобращения: 20.02.2017)
10 Saritas, S. Analysis of Android random number generator. Ph.D. Theses [Электронныйресурс] / S.Saritas, Bilkent University. 2013. 84 pp. URL: http://www.thesis.bilkent.edu.tr/0006566.pdf (Дата обращения: 20.02.2017)
11 Атака QRLJacking доказывает небезопасность авторизации с использованием SQRL [Электронный ресурс]. URL: https://xakep.ru/2016/08/02/qrljacking/ (Дата обращения: 21.12.2016).
12 В WhatsApp найдена уязвимость, позволяющая читать сообщения [Электронный ресурс].URL:https://xakep.ru/2017/01/13/whatsapp-retransmission-problem/ (Датаобращения: 15.01.2017).

REFERENCES:

[1] Telegram. Available at: https://planfix.ru/docs/Telegram (accessed 13.11.2016).
[2] Chislo pol'zovateley Telegram prevysilo 100 millionov (in Russian). Available at: https://lenta.ru/news/2016/02/23/telegram/ (accessed 13.11.2016)
[3] Secret chats, end-to-end encryption. Available at: https://core.telegram.org/api/end-to-end (accessed 13.11.2016)
[4] Jacobsen, J. B. A practical cryptanalysis of the Telegram messaging protocol. Ph.D. Theses / J. B. Jacobsen; Aarhus University: Department of Computer Science. 2015. 79 pp. Available at: https://cs.au.dk/~jakjak/master-thesis.pdf (accessed 20.02.2017).
[5] Official site of WhatsApp messenger. Available at: https://ru.wikipedia.org/wiki/WhatsApp (accessed 30.11.2016).
[6] WhatsApp Encryption Overview. Available at: https://www.whatsapp.com/security/WhatsAppSecurity-Whitepaper.pdf (accessed 30.11.2016).
[7] Cohn-Gordon, K. A Formal Security Analysis of the Signal Messaging Protocol / K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, D. Stebila. 2016. 30 pp. Available at: https://eprint.iacr.org/2016/1013.pdf (accessed 20.02.2017)
[8] Frosch, T. How secure is TextSecure? / T. Frosch, C. Mainka, C. Bader, F. Bergsma, J. Schwenk, T. Holz. 2014. 17 p. Available at: https://eprint.iacr.org/2014/904.pdf (accessed 20.02.2017)

[9] Krawczyk, H. Cryptographic Extraction and Key Derivation: The HKDF Scheme / H. Krawczyk. 2010. 34 pp. Available at: https://eprint.iacr.org/2010/264.pdf (accessed 20.02.2017)
[10] Saritas, S. Analysis of Android random number generator. Ph.D. Theses / S. Saritas, Bilkent University. 2013. 84 pp. Available at: http://www.thesis.bilkent.edu.tr/0006566.pdf (accessed 20.02.2017)
[11] Ataka QRLJacking dokazyvayet nebezopasnost' avtorizatsii s ispol'zovaniyem SQRL(in Russian). Available at: https://xakep.ru/2016/08/02/qrljacking/ (accessed 21.12.2016) (in Russian)
[12] V WhatsApp naydena uyazvimost', pozvolyayushchaya chitat' soobshcheniya(in Russian). Available at: https://xakep.ru/2017/01/13/whatsapp-retransmission-problem/ (accessed 15.01.2017)

Поступила в редакцию - 12 июня 2017 г. Окончательный вариант – 14 ноября 2017 г.
Received – June 12, 2017. The final version – November 14, 2017.

Юрий Е. Козлов, Владимир Л. Евсеев
Финансовый университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский проспект, 49, Москва, 125993, Россия
e-mail: kozlovye@yandex.ru, ORCID 0000-0002-4448-0232
e-mail: VLevseev@fa.ru, ORCID 0000-0003-3283-3106

МУЛЬТИМОДАЛЬНАЯ ТРЕХМЕРНАЯ ДИНАМИЧЕСКАЯ ПОДПИСЬ*

DOI: http://dx.doi.org/10.26583/bit.2017.4.05

Аннотация. Надежная аутентификация в мобильных приложениях является актуальнейшей задачей информационной безопасности современного общества. В настоящее время человека сложно представить без мобильного устройства, подключенного к сети internet. Кроме того, мобильное устройство может хранить большой объем конфиденциальной информации, начиная от личных фотографий, заканчивая инструментами для банковских операций. Использование жеста в воздухе в качестве методики аутентификации впервые было предложено сотрудниками Университета Райса (США) совместно с компанией Моторола в 2009 году. Эта и остальные работы по созданию и усовершенствованию данной методики указаны во введении к статье. К моменту написания статьи, программа, реализующая один из вариантов методики аутентификации при помощи жеста мобильным устройством, доступна к установке для ОС Android. Однако данная программа не получила большого распространения. Возможно, одна из причин этого - недостаточная надежность методики, которая предполагает, как и ее предыдущие аналоги, использование только одного устройства. В данной статье рассмотрена аутентификация с использованием мультимодальной трехмерной динамической подписи (МТДП), выполняемой двумя независимыми мобильными устройствами. Методика аутентификации с помощью МТДП является улучшенным вариантом аутентификации при помощи жеста в воздухе. В основной части статьи рассмотрена работа прототипа системы аутентификации на основе МТДП. Описаны основные алгоритмы, реализованные в прототипе, а так же предварительные результаты, полученные при его использовании. Авторы предполагают использование данной методики в любых мобильных приложениях после введения ряда дополнительных усовершенствований, о которых рассказано в заключении.

Ключевые слова: аутентификация, мобильное устройство, акселерометр, персонализированный жест, подпись

Для цитирования. **КОЗЛОВ, Юрий Е.; ЕВСЕЕВ, Владимир Л.** МУЛЬТИМОДАЛЬНАЯ ТРЕХМЕРНАЯ ДИНАМИЧЕСКАЯ ПОДПИСЬ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 44-51, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/276>. Дата доступа: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.05.

***Благодарности:** Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансового университета при Правительстве Российской Федерации 2017 года

Yury E. Kozlov, Vladimir L. Evseev
Financial University under the Government of the Russian Federation (Financial University),
LeningradskyProspekt, 49, Moscow, 125993, Russia
e-mail: kozlovye@yandex.ru, ORCID 0000-0002-4448-0232
e-mail: VLevseev@fa.ru, ORCID 0000-0003-3283-3106

Multimodal three-dimensional dynamic signature

DOI: http://dx.doi.org/10.26583/bit.2017.4.05

Abstract. Reliable authentication in mobile applications is among the most important information security challenges. Today, we can hardly imagine a person who would not own a mobile device

that connects to the Internet. Mobile devices are being used to store largeamounts of confidential information, ranging from personal photos to electronic banking tools. In 2009,colleagues from Rice University together with their collaborators from Motorola, proposed an authentication through in-air gestures. This and subsequent workcontributing tothe development of the method are reviewed in our introduction. At the moment, there exists a version of the gesture-based authentication software available for Android mobile devices. This software has not become widespread yet. One of likely reasons for that is the insufficient reliability of the method, which involvessimilar to its earlier analogsthe use of only one device. Here we discuss the authentication based on the multimodal three-dimensional dynamic signature (MTDS) performed by two independent mobile devices. The MTDS-based authentication technique is an advanced version of in-air gesture authentication. We describe the operation of a prototype of MTDS-based authentication, includingthe main implemented algorithms, as well as some preliminary results oftesting the software. We expect that our method can be used in any mobile application, provided a number of additional improvementsdiscussed in the conclusionare made.

Keywords: authentication, mobile device, accelerometer, personalized gestured, signature

For citation. **KOZLOV, Yury E.; EVSEEV, Vladimir L**. Multimodal three-dimensional dynamic signature. IT Security, [S.l.], v. 24, n. 4, p. 44-51, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/276>. Date accessed: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.05.

* ***Acknowledgements:*** The article is based on the results of research carried out at the expense of budget funds of the state task of the Financial University under the Government of the Russian Federation in 2017.

Введение

Аутентификация с использованием биометрических признаков способна обеспечить надежное и естественное решение задачи распознавания личности, при этом все большее исследований посвящены разработкам биометрических систем, основанных наповеденческой (динамической) характеристикечеловекаиучитывающиеособенности, характерныедляподсознательныхдвиженийчеловекавпроцессевоспроизведениякакого-либодействия. Это связано с тем, что неизменяемость и открытость биометрических характеристик, используемых в статических методах, в отличие от динамических, допускают подделку биометрического ключа [1].

Биометрические идентификаторы практически неотторжимы от субъекта и присущи только ему и никому другому, поэтому ими почти невозможно манипулировать. Принципиально важным преимуществом динамических биометрических систем контроля доступа является возможность для личности сохранять в тайне свой биометрический образ, что повышает степень защиты относительно статических биометрических систем контроля доступа [2].

Одной из причин сдерживающих внедрение биометрической аутентификации на практике, является требование соблюдения строгих правил при защите персональных данных, закрепленного в законодательных актах различных стран. Одним из примеров является принятый в 2016 году новый регулирующий акт GlobalDataProtectionRegulation (GDPR), регулирующий защиту персональных данных граждан стран-членов Европейского Союз, в котором биометрические идентификаторы признаны персональными данными, и правила их обработки строго регламентируются[3].

Использование МТДП для аутентификации в мобильных приложениях

Мультимодальная трехмерная динамическая подпись основана на использовании специального жеста для аутентификации. Работы по созданию методик аутентификации при помощи жеста проводились Университетом Райса (США) совместно с компанией Моторола [4,5], а так же Политехническим университетом Мадрида (CeDInt-UPM) (Испания) [6].Кроме того, приложение «InAirSignature», реализующее разблокировку телефона при помощи жеста, доступно для бесплатной установки в операционной системы (ОС) Android.

Появление умных часов и фитнес браслетов позволили значительно повысить надежность методик аутентификации за счет одновременного использования двух независимых устройств одновременно [7]. Поскольку такая аутентификация будет иметь схожесть с рукописной подписью по своим динамическим свойствам (биометрические особенности воспроизведения по скорости и амплитуде), а так же будет содержать два источника данных (мобильное и запястное устройство), можно назвать такой способ - мультимодальная трехмерная динамическая подпись (далееМТДП).

Такая подпись, как и в случае рукописной подписи, потребует выработки специфического функционально-динамического комплекса навыков(ФДК), представляющего собой явление психофизиологической природы, сущность которого составляет система навыков, предназначенных для целевой реализации определенных действий.

МТДП с целью повышения надежности аутентификации предполагает при воспроизведении жеста, регистрацию его двумя устройствами одновременно – мобильным и запястным.

На рисунке 1 представлен пример МТДП, точкой обозначено начало траектории, а стрелкой указывается ее направление.

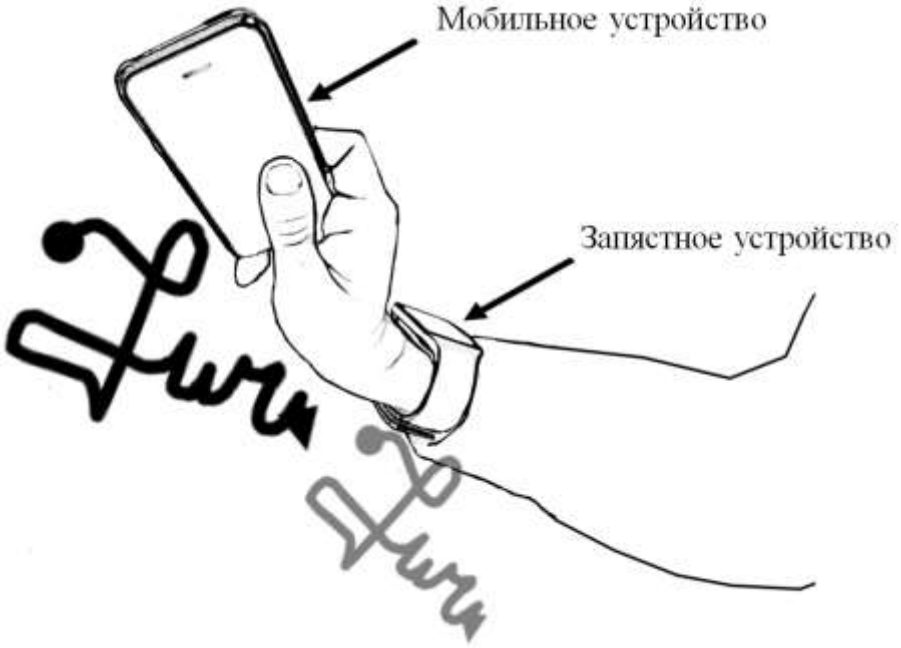


Рисунок 1 -Пример реализации мультимодальной трехмерной динамической подписи с использованием двух устройств
(Fig. 1-Example implementation of multimodal three-dimensional dynamic signature using two devicesЪ

Для «парольного» жеста подойдет любой жест, который человек сможет запомнить и впоследствии воспроизводить.

Процедура выработки эталона для МТДП схожа с процедурой подпись на бумажных документах. Пользователь сам определяет понравившийся ему вариант. И для закрепления навыков и выработки порога срабатывания повторяет его несколько раз (в разработанной реализации используется три попытки). При этом система определят разброс в воспроизведении МТДП и устанавливает порог срабатывания.

Неоспоримым преимуществом МТДП, как системы использующей динамические биометрические признаки, является легкая система смены признака и уточнение его порогов. Кроме того процесс аутентификации легко скрыть, даже используя его в людных местах. Для этого необходимо выбрать в качестве жеста, любой неприметный жест, который не вызовет подозрений. Проведенные предварительные исследования, а так же

исследования, представленные для аналога, показывают, что даже снятый на видео жест тяжел для точного воспроизведения другим человеком [5].

В таблице 1 представлено влияние внешних факторов на МТДП и распространенные системы биометрической аутентификации.

Таблица 1

Методика	**Влияниевнешнихфакторов**			
	Плохаяосвещенность	Шумноеместо	Низкаятемпература	Высокаятемпература
Отпечатокпальца	нет	нет	среднее	среднее
Распознаваниелица	**высокое**	нет	низкое	низкое
Речеваяаутентификация	нет	**высокое**	нет	нет
Радужнаяоболочкаглаза	**высокое**	нет	нет	нет
МТДП	нет	нет	нет	нет

Из таблицы видно, что МТДП имеет лучшую применяемость в шумном месте с плохой освещенностью. Стоит отметить, что в условиях городских улиц это очень частая ситуация.

Работа системы аутентификации на базе МТДП предполагает этап формирования подписи МТДП. На рисунке 2 представлен укрупненный алгоритм работы прототипа системы формирования МТДП, реализованный на базе ОСАндройд.

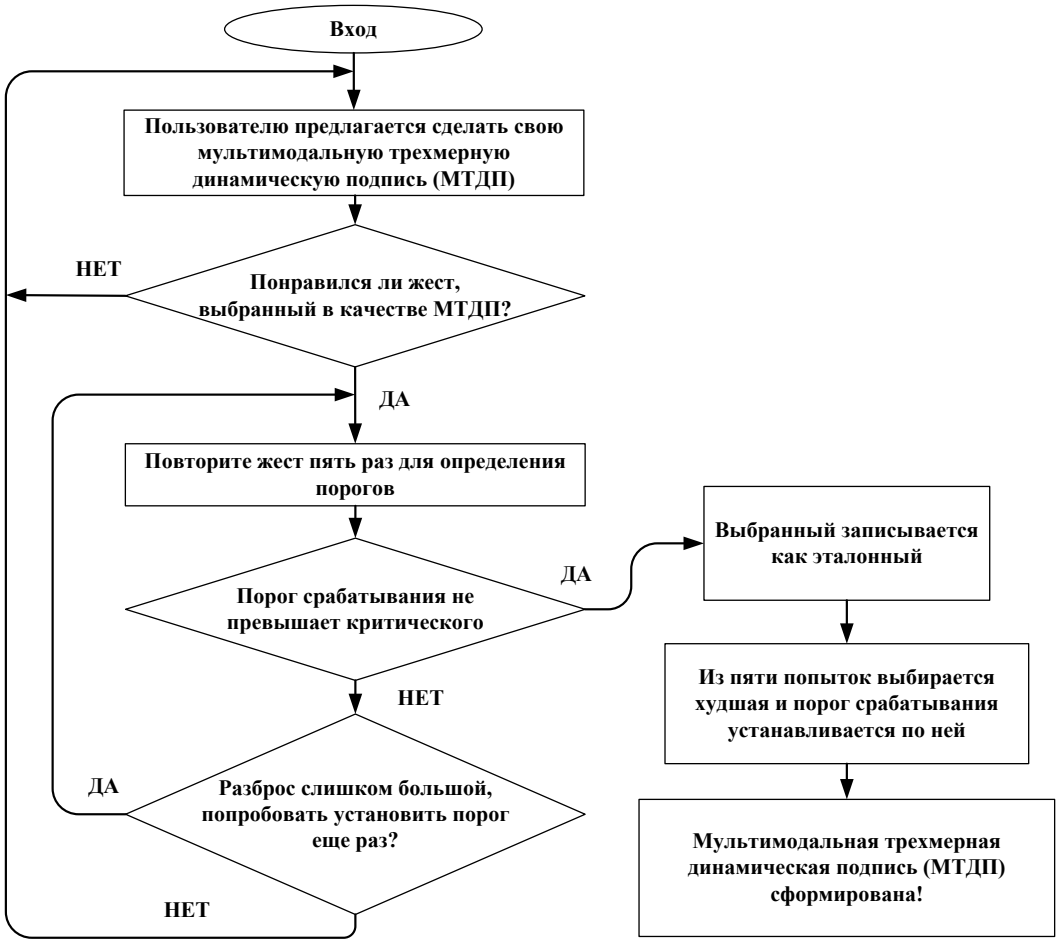


Рисунок 2 - Алгоритм формирования МДТП
(Fig. 2- Algorithm of formation MDTP)

После того, как МТДП сформирована, система готова к работе. Сама процедура аутентификации предполагает использование трех попыток для аутентификации. Если хотя бы одна из трех попыток соответствует шаблону с точностью, не превышающей порога, то аутентификация считается пройденной.

Укрупненный алгоритм процедуры аутентификации, реализованный в прототипе, представлен на рисунке 3.

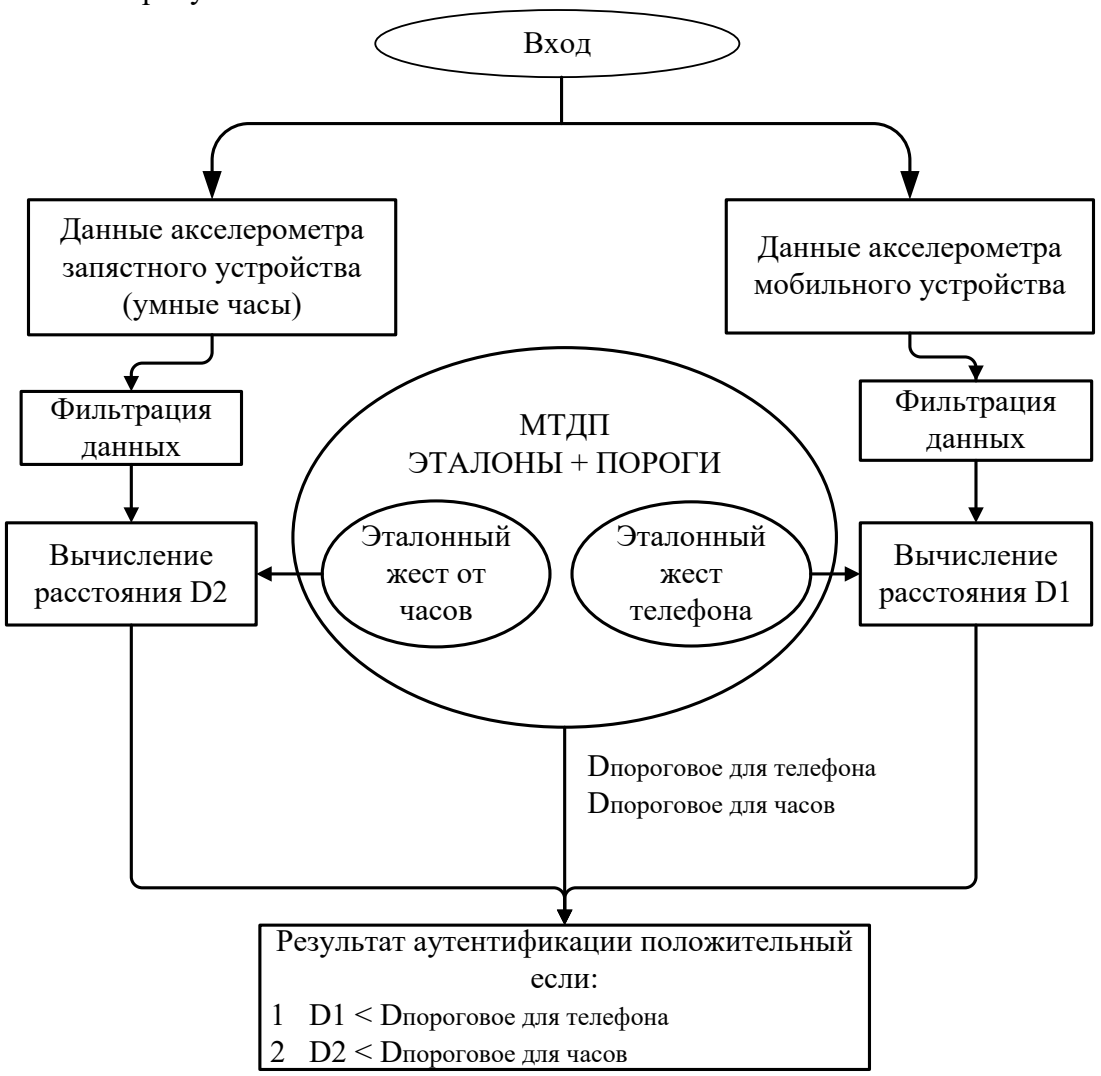


Рисунок 3 -Работа системы аутентификации на базе МТДП
(Fig. 3 - System-based authentication MTDP)

Данные акселерометров устройств участвующие в формировании МТДП и аутентификации являются временными рядами и для нахождения меры близости на всех шагах, где это требуется, используется алгоритм трансформации временного ряда (DTW). Допустим имеется эталон $Q=(q_1,q_2\ldots q_n)$ и воспроизведенный жест $C=(c_1,c_2\ldots c_m)$, суть алгоритма DTW заключается в вычислении минимального пути W по формуле (1) [8]:

$$DTW(Q,C) = min\left\{\frac{\sum_{k=1}^{k} d(w_k)}{K}\right\} \quad (1),$$

где:
K - длина пути,
$d(w_k) =(q_i-c_j)^2$ - элемент пути.

Прототип МТДП был опробован на нескольких современных смартфонах, время, необходимое программе для расчетов и принятия решения об аутентификации, для

пользователя кажется незаметным, это позволяет сделать вывод, что алгоритм с точки зрения производительности выбран правильно.

Создание прототипа системы аутентификации на базе МТДП позволило запланировать эксперимент для того, чтобы получить количественные оценки надежности системы.

В качестве показателей, характеристики которых должен определить эксперимент, являются ошибки первого FRR – вероятность отказа доступа человеку, имеющему доступ и второго рода FAR – вероятность ложного пропуска человека, не имеющего доступ.

Доверительный интервал для предварительной оценки точности ошибок можно определить по следующей формуле (2) [9].

$$p = \frac{n}{g^2+n}\left(\omega + \frac{g^2}{2n} \pm g\sqrt{\frac{\omega(1-\omega)}{n} + \frac{g^2}{4n^2}}\right) \quad (2),$$

Параметр g определяется уровнем доверительной вероятности на основе функции Лапласа. При уровне равном 0.95 параметр g = 1.96.

Предварительные результаты показали, чторост точности за счет использования двух устройств составил примерно 30 %. При этом были проанализированы 1500 попыток аутентификации, проводимой девятью различными людьми.

На рисунке 4 представлен анализ попыток аутентификация для одного из пользователей.

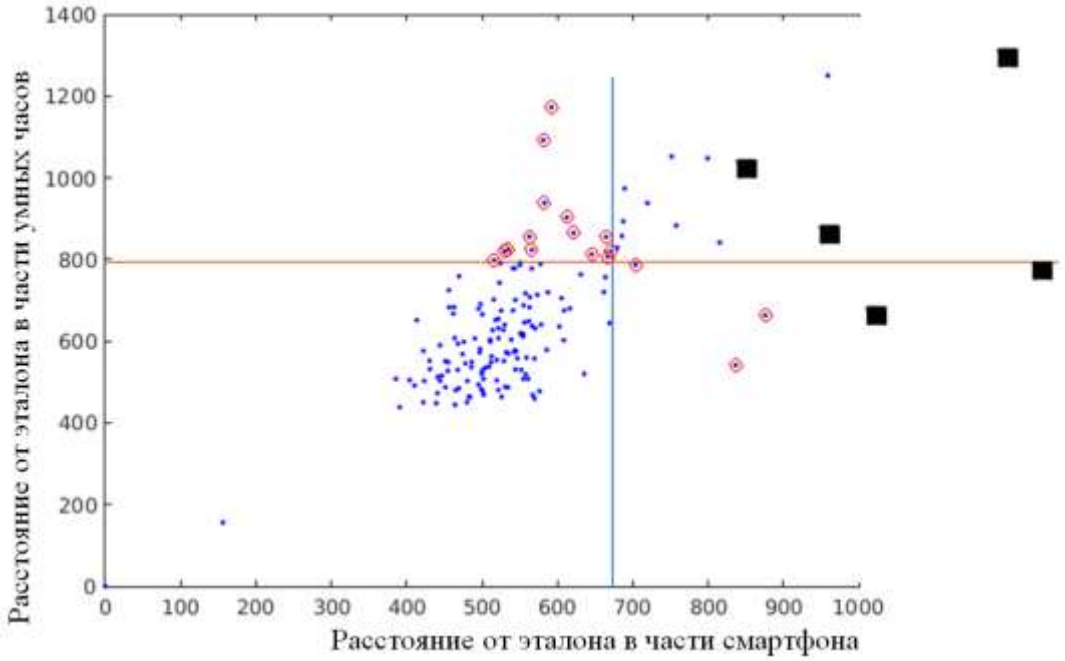


Рисунок4 - Анализ попыток аутентификации
(Fig. 4 - Analysis of authentication attempts)

По оси абсцисс на рисунке 4 отложены, полученные при помощи алгоритма DTW, расстояния между эталонной МТДП и воспроизведенной в части смартфона, а по оси ординат аналогичное расстояние для умных часов. Линии на рисунке - это пороги (уровни, выше которых происходит отсечение) для смартфона (вертикальная линия) и умных часов (горизонтальная линяя). Попытки, отсеченные (не прошедшие аутентификацию) только одним из устройств, обведены кружками. Квадраты на рисунке – попытки воспроизвести жест другим человеком, который видит воспроизведение жеста автором (попытки взлома).

Предварительнаяоценкачастотыошибокпервогоивторогородаможетбытьнайденаисхо дяизанализаошибоканалогов, учетом увеличения точности на 30%, и будет составлять для ошибок первого рода ω_1=0.025 и второго рода и ω_2=0.025 [5,6].

Для получения достоверных данных о надежности системы запланировано не менее 4000 экспериментовопределения вероятности ошибок первого рода и не менее 1000 экспериментовдля определения вероятности ошибок второго рода.

Подставляяэти данные в формулу(2), получаемпредварительныеграницыдоверительныхинтерваловдляошибокпервогоивторогорода: $p_1 \in [0.02; 0.03]$ и$p_2 \in [0.016; 0.036]$. Данныйрасчетявляется прикидочным, посколькусамихоцениваемыхвероятностейпоканет, однакопорядокоценкиточностиэтихзначенийнеизменится.

Основной проблемой МТДП и его предыдущих аналогов, так же как и у систем аутентификации на основе рукописной подписи, является выработка человеком ФДК, необходимого для достаточно точного воспроизведения подписи. Кроме того, сложность самой подписи тоже имеет решающее значение. Так, например, если в качестве МТДП, будет выбран просто круг в воздухе, то надежность такой подписи может быть поставлена под сомнение. В связи с этим МТДП будет дорабатываться системой оценки подписи, которая будет определять надежность, с учетом полученных порогов, а так же давать рекомендации пользователям о возможности ее применения.

Заключение

Система аутентификации личности на основе МТДП, реализованная в мобильных приложениях, обладает перспективами применения в условиях повышенного уровня акустического шума или плохого освещения, а также как вспомогательная методика аутентификации. Надежность системы позволяет использовать ее для всех типов мобильных приложений, где может требоваться аутентификация.

СПИСОК ЛИТЕРАТУРЫ:

1 Брагина Е. К., Соколов С. С. «Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития». ISSN 1812-9498. Вестник АГТУ. 2016 г. № 1 (61). С. 40-45.
2 ГОСТ Р 52633.0-2006. Национальный стандарт российской федерации защита информации техника защиты информации требования к средствам высоконадежной биометрической аутентификации. М.: Стандартинформ, 2007, 24 с.
3 Regulation (EU) 2016/679 of the european parliament and of the council, 2016. URL:http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (Дата обращения: 05.09.2017 г.).
4 Jiayang L., Zhen W., Lin Z., Jehan W., Venu V. «Wave: Accelerometer-based Personalized Gesture Recognition and its Applications». 2009. URL:http://www.ruf.rice.edu/~mobile/publications/liu09percom.pdf. (Дата обращения: 24.03.2017 г.).
5 Jiayang L., Lin Z., Jehan W., Venu V. «User Evaluation of Lightweight User Authentication with a Single Tri-Axis Accelerometer». 2009. URL:http://www.ruf.rice.edu/~mobile/publications/liu09mobilehci.pdf (Дата обращения: 24.03.2017 г.).
6 JavierGuerra-Casanova, CarmenSánchez-Ávila, GonzaloBailador-delPozo, AlbertodeSantos «ApplicationofLCSAlgorithmtoAuthenticateUserswithinTheirMobilePhoneThroughIn-AirSignatures». URL:https://www.intechopen.com/books/advanced-biometric-technologies/application-of-lcs-algorithm-to-authenticate-users-within-their-mobile-phone-through-in-air-signatur (Датаобращения: 06.09.2017 г.).
7 Козлов Ю.Е., Евсеев В.Л. «Метаматематическая модель мультимодальной жестовой аутентификации при помощи двух независимых мобильных устройств». Безопасность информационных технологий. 2017 г., №1, С. 49-55.
8 Herbst N. R. «Quantifying the Impact of Platform Configuration Space for Elasticity Benchmarking». Karlsruhe Institute of Technology. StudyThesis, 2011, 93 p.
9 Б.Л. ван дер Варден «Математическая статистика». Издательство иностранной литературы. Перевод с немецкого Л.Н. Большева, 1957 г., 435 с.

REFERENCES:

[1] Bragina E. K., Sokolov S. S. Modern methods of biometric authentication: a review, analysis and definition of prospects of development. ISSN 1812-9498. Vestnik AGTU. 2016. № 1 (61). P. 40-45. (in Russian).
[2] GOST R 52633.0-2006 Nacional'nyj standart rossijskoj federacii zashhita informacii tehnika zashhity informacii trebovanija k sredstvam vysokonadezhnoj biometricheskoj autentifikacii. M.: Standartinform, 2007, 24 p. (in Russian).

[3] Regulation (EU) 2016/679 of the european parliament and of the council, 2016. URL:http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (accessed 05.09.2017).
[4] Jiayang L., Zhen W., Lin Z., Jehan W., Venu V. «Wave: Accelerometer-based Personalized Gesture Recognition and its Applications». 2009. URL:http://www.ruf.rice.edu/~mobile/publications/liu09percom.pdf. (accessed 24.03.2017).
[5] Jiayang L., Lin Z., Jehan W., Venu V. «User Evaluation of Lightweight User Authentication with a Single Tri-Axis Accelerometer». 2009. URL:http://www.ruf.rice.edu/~mobile/publications/liu09mobilehci.pdf (accessed 24.03.2017).
[6] Javier Guerra-Casanova, Carmen Sánchez-Ávila, Gonzalo Bailador-del Pozo, Alberto de Santos «Application of LCS Algorithm to Authenticate Users within Their Mobile Phone Through In-Air Signatures» URL:https://www.intechopen.com/books/advanced-biometric-technologies/application-of-lcs-algorithm-to-authenticate-users-within-their-mobile-phone-through-in-air-signatur (accessed 06.09.2017).
[7] Kozlov Y. E., Evseev V. L. «Metamathematics model multimodal gestural authentication with two independent mobile devices». Bezopasnost' informacionnyh tehnologij. 2017, №1, P. 49-55. (in Russian).
[8] Herbst N. R. «Quantifying the Impact of Platform Configuration Space for Elasticity Benchmarking». Karlsruhe Institute of Technology. Study Thesis, 2011, 93 p.
[9] B.L. van der Varden «Mathematical statistics». Izdatel'stvo inostrannoj literatury. Translated from the German by L. N. Bolsheva 1957, 435 p.(in Russian).

Поступила в редакцию - 01 июля 2017 г. Окончательный вариант – 01 ноября 2017 г.
Received – Jule 01, 2017. The final version – November 01, 2017.

Александр В. Кузнецов
Финансовый университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский проспект, 49, Москва, 125993, Россия
e-mail: a.kuznetsov@ntc-vulkan.ru, ORCID0000-0002-7160-1845

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМИЧЕСКОГО АППАРАТА УПРАВЛЕНИЯ СОБЫТИЯМИ БЕЗОПАСНОСТИ И РЕЗУЛЬТАТЫ ЕЕ ПРИМЕНЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2017.4.06

Аннотация. В настоящей статье рассматривается актуальная задача в области защиты информации, обусловленная отсутствием алгоритмического аппарата управления событиями безопасности и автоматизации процедур определения набора регистрируемых событий безопасности. В первой части статьи сформулирована постановка математической задачи, подлежащей автоматизации с использованием табличного процессора, в том числе определена целевая функция и её переменные, а также приведены ссылки на источники, содержащие сведения о самом алгоритме решения. Представлено писание предложенного автором программного модуля, реализующего алгоритм определения набора регистрируемых событий безопасности, разработанного на базе табличного процессора, сертифицированного по требованиям безопасности информации Федеральной службой по техническому и экспортному контролю. Представлено описание контрольного примера, подготовленного для тестирования разработанного программного модуля, размерностью 30х20, содержащего 14 вариантов пороговых значений количества зарегистрированных событий безопасности варьировалось. Результаты применения программного модуля подтвердили соблюдение заданных граничных условий задачи, выявили нелинейную зависимость целевой функции от увеличения количества регистрируемых событий безопасности, а также нелинейную зависимость процента регистрируемых событий безопасности от общего исходного количества событий безопасности, подлежащих регистрации на источнике событий. Оценка производительности применения предложенного программного модуля, а именно загрузки центрального процессора, являлась приемлемой (не превысила 33%), что позволяет применять данную программную реализацию для типовых автоматизированный рабочих местах специалистов по защите информации, оснащенных соответствующими табличными процессорами. Предложенный в статье подход к программной реализации различных алгоритмов может быть инвариантен к области применения.

Ключевые слова: событие безопасности, управление событиями безопасности, SIEM, источник событий, табличный процессор

Для цитирования. **КУЗНЕЦОВ, Александр В**. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМИЧЕСКОГО АППАРАТА УПРАВЛЕНИЯ СОБЫТИЯМИ БЕЗОПАСНОСТИ И РЕЗУЛЬТАТЫ ЕЕ ПРИМЕНЕНИЯ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 52-59, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/277>. Дата доступа: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.06.

Aleksandr V. Kuznetcov
Financial University under the Government of the Russian Federation(Financial University),
Leningradsky prospect, 49, Moscow, 125993, Russia
e-mail: a.kuznetsov@ntc-vulkan.ru, ORCID 0000-0002-7160-1845

Software for security event management:Development and utilization

DOI: http://dx.doi.org/10.26583/bit.2017.4.06

Abstract. We address the challenge to the information security coming from the lack of algorithmic machinery for managing the security events. We start with a mathematical formulation of the problem for a tabular processor by introducing an appropriate target function. Details of corresponding algorithm can be found by following the provided links. We describe our original software module that implements the algorithm for determining the registered security events. The module is based on the tabular processor certified by the Russian Federal Service for Technical and Export Control. We present a control sample for testing the developed module. The sample has the dimension 30x20 and contains 14 choices for threshold values of security events number. The results of the tests comply with the specified boundary conditions and demonstrate a nonlinear dependence of the objective function onthe number of registered security events, as well as a nonlinear dependence of the percentage of the detected security event on the total initial number of security events to be registered at the event source. The performance of the module specifically, the central processing unit usage is found acceptable (not exceeding 33%), which allows one to use the software for typical automated workplaces equipped with appropriate tabular processors. Our approach is universal with respect to the application areas.

Keywords: security event, security event management, SIEM, event source, tabular processor
For citation. **KUZNETCOV, Aleksandr V.** Software for security event management: Development and utilization. IT Security, [S.l.], v. 24, n. 4, p. 52-59, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/277>. Date accessed: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.06.

Введение

Вопросы защиты информации не только не теряют своей актуальности на протяжении ряда десятилетий, но и стремительно развиваются и выходят на один из первых планов в научно-практической деятельности в последние годы. Системы управления информационной безопасностью становятся неотъемлемой частью систем управления современных организации и предприятий наравне с системами управления качеством и охраной труда. Управление событиями безопасности является одним из основополагающих процессов управления в рамках систем управления информационной безопасностью. Составной частью процесса управления событиями безопасности является регистрация событий безопасности [1-2]. Принимая во внимание, что современные источники событий, а именно программное и программно-аппаратное обеспечение, способные вести журнал аудита, имеют возможности по регистрации сотен и в ряде случаев тысяч различных событий безопасности, возникает необходимость формирования алгоритмического аппарата управления событиями безопасности и автоматизации процедур определения набора регистрируемых событий безопасности. На сегодняшний день в полном объеме данная задача не решена [3-5].

В настоящей статье рассматривается вариант программной реализации алгоритмического аппарата управления событиями безопасности в рамках системы управления информационной безопасностью с использованием табличного процессора, а также результаты работы данной программной реализации на базе контрольного примера.

Алгоритмический аппарат управления событиями безопасности

В ряде публикаций автором был предложен алгоритмический аппарат управления событиями безопасности в рамках системы управления информационной безопасностью [6,7], а именно алгоритм выбора набора регистрируемых событий безопасности E, которому однозначно соответствует набор булевых переменных e, из полного набора событий безопасности, подлежащих регистрации на источнике событий, при заданной в системе класса Security Information and Event Management (далее – SIEM-системе) базе

знаний, т.е. корреляционных правил I, и ограничении на производительность источника событий, который обращал бы в максимум целевую функцию W (1).

$$W = \sum_{j=1}^{m} I_j = \sum_{j=1}^{m} \sum_{i=1}^{n} b_{ij} \cdot e_i = \sum_{i=1}^{n} (\sum_{j=1}^{m} b_{ij}) \cdot e_i \rightarrow \max \quad (1),$$

где:

Ij – корреляционное правило из SIEM-системы;

m – количество корреляционных правил в SIEM-системы;

n – количество событий безопасности;

bij – нормирующий коэффициент, соответствующий вхождению i-ого события безопасности ei в j-ое корреляционное правило Ij.

ei – дискретная величина, соответствующая данным из набора событий безопасности E, которые могут быть зарегистрированы источником событий.

Алгоритм основан на публикациях, посвященных решению задач поиска экстремума [8-10], а также применению табличных процессоров для автоматизации решения подобных задач [11-13].

Программная реализация

Программный модуль, реализующий предложенный алгоритм, был разработан автором на базе табличного процессора. В качестве табличного процессора выступает 64-разрядная версия программного обеспечения «MicrosoftExcel 2013», входящего в программный пакет «MicrosoftOffice профессиональный плюс 2013», сертифицированный по требованиям безопасности информации ФСТЭК России [14], далее – MicrosoftExcel.
Для инсталляции, запуска и использования на автоматизированном рабочем месте программного модуля данное место должно удовлетворять следующим требованиям [15]:

частота центрального процессора не ниже 1 ГГц;
оперативная память не менее 2 Гбайт;

свободное место на жестком диске не менее 3 Гбайт;

экран с расширением не ниже 1 024 X 576;

64-разрядная операционная система не ниже MicrosoftWindows 7.

Указываемые оператором программного модуля параметры поиска решения приведены на рисунке ниже (см. рис.1). Форма представления результатов работы программного модуля приведена на рисунке ниже (см. рис. 2).

Контрольный пример

Для тестирования программного модуля автором был подготовлен контрольный пример, содержащий следующие исходные данные:

количество событий n = 30;

количество корреляционных правил m= 20;

матрицакоэффициентов b_{ij} (в каждом корреляционном правиле участвует 3 события безопасности);

матрицакоэффициентов a_{ij} (в каждой ячейке указано случайное число в интервале от 100 до 500);

пороговое значение количества зарегистрированных событий безопасности варьировалось (14 значений), но не превышало максимального значения: 10 135 событий.

Обобщенные результаты тестирования в рамках контрольного примера представлены в таблице ниже (см. Таблица 1).

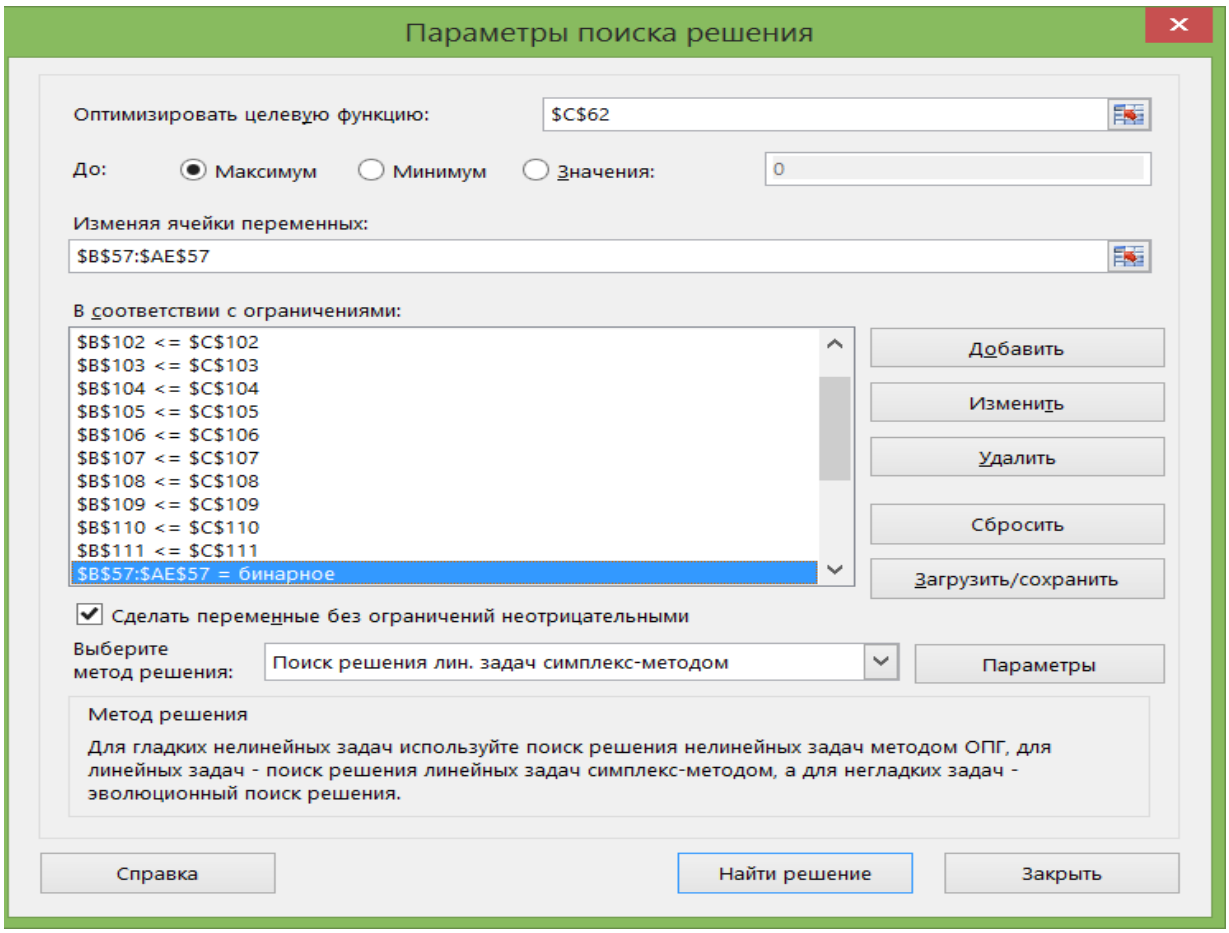


Рисунок 1 - Устанавливаемые параметры поиска решения
(Fig. 1 - Set parameters of the search decision)

Рисунок 2 - Представление результатов
(Fig. 2 - Presentation of the results)

Таблица 1. Результатытестирования в рамках контрольного примера

№ п.п.	*L*	*N*	*n*	*n/N*	*W*
1	2	3	4	5	6
1.	10 135	30	30	1,00	20
2.	10 000	30	29	0,97	18
3.	9 500	30	28	0,93	16
4.	9 000	30	27	0,90	14
5.	8 500	30	26	0,87	12
6.	8 000	30	24	0,80	10
7.	7 500	30	23	0,77	6
8.	7 000	30	21	0,70	6
9.	6 500	30	20	0,67	6
10.	6 000	30	19	0,63	5

№ п.п.	*L*	*N*	*n*	*n/N*	*W*
1	2	3	4	5	6
11.	5 500	30	17	0,57	4
12.	4 500	30	14	0,47	4
13.	3 500	30	11	0,37	2
14.	2 000	30	6	0,20	0

Зависимость *W(n)* представлена на рисунке ниже (Рисунок 3), где $W_{max} = 20$, $n_{max} = 30$.

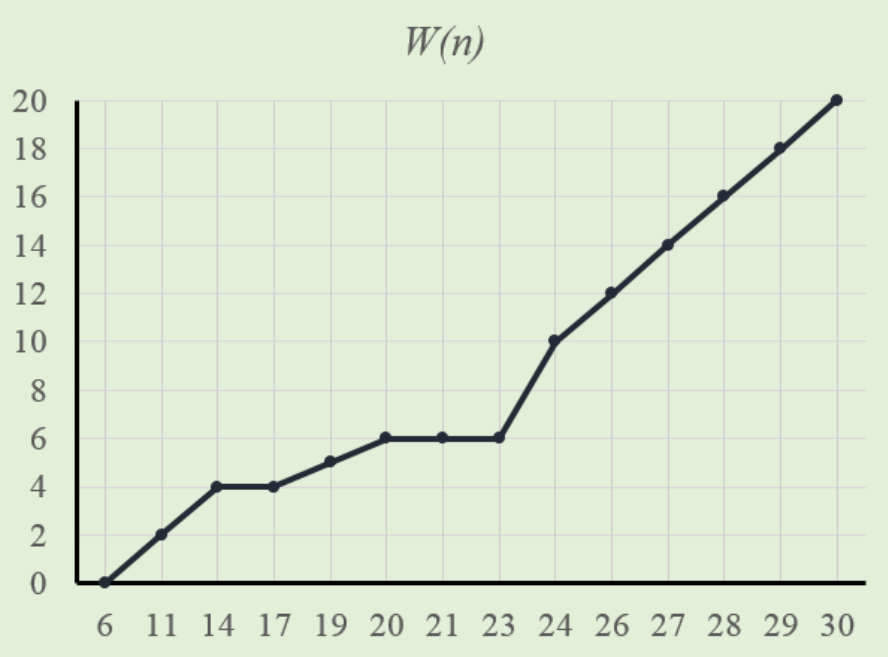


Рисунок 3 - Значения целевой функции в рамках контрольного примера
(Fig. 3 - Values of the objective function to the control example)

Зависимость *n/N(L)* представлена на рисунке ниже (Рисунок 4).

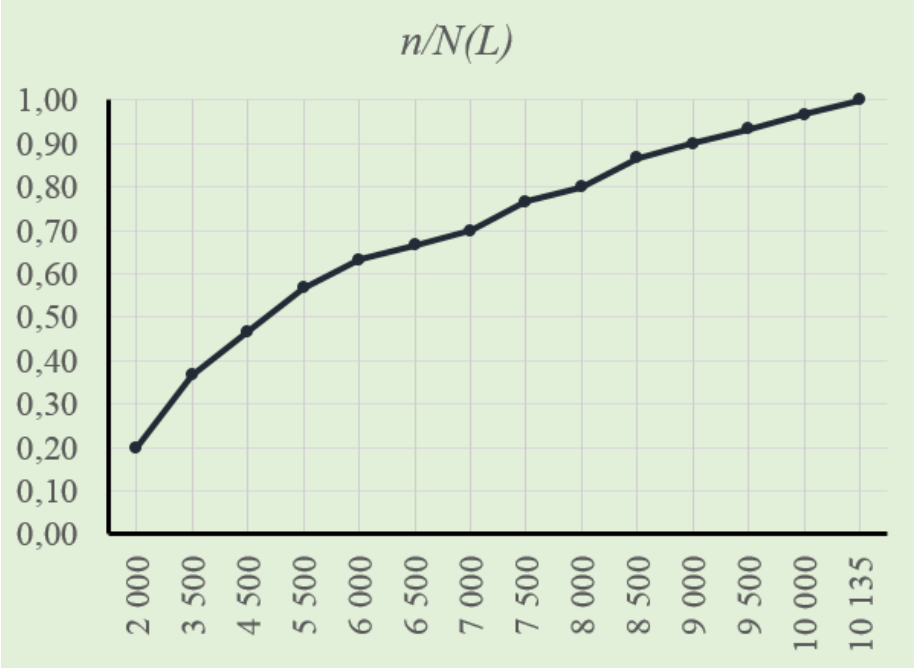


Рисунок 4 - Процент выборки событий в рамках контрольного примера
(Fig. 4 - Percentage of sampling events in the control sample)

Заключение

Результаты применения программного модуля показали, что:

выполняются граничные условия задачи, т.е. при $L = 10\,135, W = 20$, что подтверждает корректность работы алгоритма определения набора регистрируемых событий безопасности;

величина целевой функции W с увеличением количества регистрируемых событий безопасности возрастает нелинейно;

процент регистрируемых событий безопасности от общего исходного количества n/N с увеличением порогового значения L возрастает нелинейно.

При выполнении вычислений загрузка центрального процессора с IntelCorei7 с тактовой частотой 2 ГГц тестовой автоматизированной рабочей станции не превысила 33% (см. рис.5), что позволяет применять разработанную программную реализация алгоритма определения набора регистрируемых событий на типовых автоматизированный рабочих местах специалистов по защите информации, оснащенных табличным процессором MicrosoftExcel.

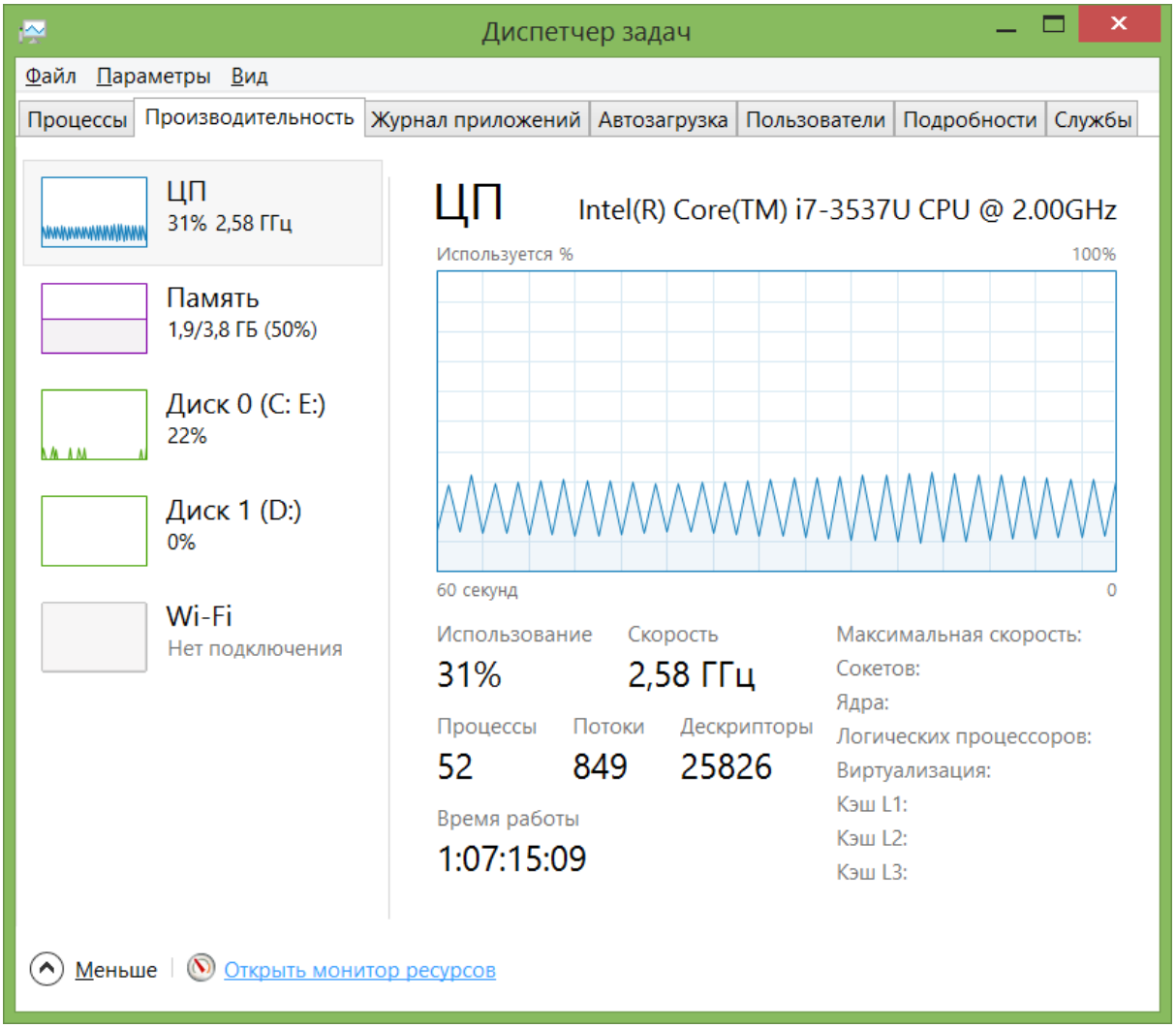


Рисунок 5 - Статистика загрузки центрального процессора при выполнении вычислений контрольного примера
(Fig. 5 - Statistics of the CPU usage while performing calculations control example)

Стоит отметить, что предложенный автором подход к программной реализации алгоритмов решения задач поиска экстремума является инвариантным к области его применения, что позволяет применять его специалистам в различных областях и сферах науки и жизнедеятельности.

СПИСОК ЛИТЕРАТУРЫ:

1 Кузнецов, А.В. Способ организации процесса управления событиями, в части их обработки, в рамках системы управления информационной безопасностью предприятия [Текст] А.В. Кузнецов. Вопросы защиты информации. - 2015. - N 2. - С.57–62.
2 ITILServiceOperation [Текст]: secondedition. - AXELOS. - 2011. - С.58-72.
3 Roer, K. BuldingaSecurityCulture [Текст] K. Roer. - IT Governance Publishing. – 2015. - 74 p.
4 Журналирование событий на маршрутизаторе Cisco (cisco log syslog aaa accounting snmp monitoring) [Электронный ресурс]. – Режим доступа: http://www.opennet.ru/base/cisco/cisco_logging.txt.html
5 Oltsic, J. An Analytics-based Approach to Cybersecurity [Текст] J. Oltsic. - The Enterprise Strategy Group, Inc. - 2015, may. - 4 p.
6 Кузнецов, А.В. Способ определения регистрируемых событий [Текст]. А.В. Кузнецов Вопросы кибербезопасности. - 2015. - N 5 (13). - С.23-25.
7 Кузнецов, А.В. Способ определения событий, регистрируемых в журналах аудита [Текст]. А.В. Кузнецов Безопасность информационных технологий (IT Security). ISSN 2074-7128. - М., Том 23, N 1(2016). - С.59-63.
8 Вентцель, Е.С. Исследование операций: задачи, принципы, методология [Текст]: 2-е изд. Е.С. Вентцель. - М: Наука. - 1988. - С.80-81.
9 Сигал, И.Х. Введение в прикладное дискретное программирование: модели и вычислительные алгоритмы [Текст] И.Х. Сигал, А.П. Иванова. - М: ФИЗМАТЛИТ. - 2002. - С.19, 22-25.
10 Nurminski, E.A. Single-projection procedure for linear optimization. Journal of Global Optimization [Текст] E.A. Nurminski DOI: 10.1007/s10898-015-0337-9. - 2015. - С.1-3.
11 Smith, N. Linear Programming Using Excel [Текст] N. Smith. - 2010. - С.1-7.
12 Данилин, Г.А. Математическое программирование с EXCEL [Текст]: учеб. пособие для студентов всех спец-й МГУЛа Г.А. Данилин. - М: [МГУЛ], 2005. - С.11-15.
13 Гераськин, М.И. Линейное программирование. Выполнение расчетов в табличном процессоре Excel [Текст]: учеб. пособие М.И. Гераськин. – Самара: Изд-во Самар. гос. аэрокоун-та. - 2012. - С.74-88
14 Сертифицированные продукты Microsoft [Электронный ресурс]. – Режим доступа: https://www.microsoft.com/ru-ru/securitycertification/products.aspx.
15 Требования к системе для Office 2013 [Электронный ресурс]. – Режим доступа: https://technet.microsoft.com/ru-ru/library/ee624351.aspx.

REFERENCES:

[1] Kuznecov, A.V. Method of organization of the event management process, in terms of their treatment in the framework of information security management of the enterprise. Voprosy zashhity informacii. - 2015. - N 2. - P.57–62. (in Russian)
[2] ITIL Service Operation: second edition. - AXELOS. - 2011. - P.58-72.
[3] Roer, K. Bulding a Security Culture. K. Roer. - IT Governance Publishing. – 2015. - 74 p.
[4] Cisco log syslog aaa accounting snmp monitoring. Available at: http://www.opennet.ru/base/cisco/cisco_logging.txt.html.
[5] Oltsic, J. An Analytics-based Approach to Cybersecurity. J. Oltsic. - The Enterprise Strategy Group, Inc. - 2015, may. - 4 p.
[6] Kuznecov, A.V. The method of determining the recorded events. Voprosy kiberbezopasnosti. - 2015. - N 5 (13). - P.23-25. (in Russian).
[7] Kuznecov, A.V. The method of determining the events recorded in the audit logs. Bezopasnost' informacionnyh tehnologij (IT Security). ISSN 2074-7128. - M., v.23, N1(2016). - P.59-63. (in Russian).
[8] Ventcel', E.S. Operations research: tasks, principles, methodology: 2-e izd. E.S. Ventcel'. - M: Nauka. - 1988. - P.80-81. (in Russian).
[9] Sigal, I.H. Introduction to applied discrete programming: models and computing algorithms. I.H. Sigal, A.P. Ivanova. - M: FIZMATLIT. - 2002. - P.19, 22-25. (in Russian)
[10] Nurminski, E.A. Single-projection procedure for linear optimization. Journal of Global Optimization. E.A. Nurminski. DOI: 10.1007/s10898-015-0337-9. - 2015. - P.1-3.
[11] Smith, N. Linear Programming Using Excel. N. Smith. - 2010. - P.1-7.
[12] Danilin, G.A. Mathematical programming with EXCEL [Tekst]: ucheb. posobie dlja studentov vseh spec-j MGULa G.A. Danilin. - M: [MGUL], 2005. - P.11-15. (in Russian).
[13] Geras'kin, M.I. Linejnoe programmirovanie. Vypolnenie raschetov v tablichnom processore Excel: ucheb. posobie M.I. Geras'kin. – Samara: Izd-vo Samar. gos. ajerokoun-ta. - 2012. - P.74-88 (in Russian).

[14] Certified Microsoft products. Available at: https://www.microsoft.com/ru-ru/securitycertification/products.aspx.
[15] System requirements for Office 2013. Available at: https://technet.microsoft.com/ru-ru/library/ee624351.aspx.

Поступила в редакцию - 29 июня 2017 г. Окончательный вариант – 12 ноября 2017 г.
Received – June 29, 2017. The final version – November 12, 2017.

Сергей Б. Козлачков[1], Андрей М. Бонч-Бруевич[1], Сергей В. Дворянкин[2],
Надежда В. Васильевская[3], Александра Л. Селенина[1]
[1]Московский Государственный Технический Университет им. Баумана,
2-я Бауманская, 5, Москва, 105005, Россия
e-mail: ksb.perovo@mail.ru, ORCID 0000-0002-7096-6711
e-mail: 123andryb@mail.ru, ORCID 0000-0002-4453-2979
e-mail: so.zz.va@yandex.ru,ORCID 0000-0002-4280-8214
[2]Финансовый Университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский проспект, 49, Москва, 125993, Россия
e-mail: SVDvoryankin@fa.ru, ORCID 0000-0001-6908-0676
[3]ФСТЭК России, Старая Басманная ул., 17, Москва, 105066, Россия
e-mail: infuzoriavalenoc@yandex.ru, ORCID 0000-0002-0078-8665

НЕКОТОРЫЕ ОСОБЕННОСТИ ФОРМИРОВАНИЯ АКУСТОЭЛЕКТРИЧЕСКОГО КАНАЛА УТЕЧКИ РЕЧЕВОЙ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2017.4.07

Аннотация. В статье рассмотрены актуальные вопросы оценки защищенности акустоэлектрического канала утечки речевой акустической информации, обусловленные различными физическими принципами функционирования разных типов электромеханических преобразователей.

Проведен анализ возможностей технических средств и методов, используемых при ведении акустической речевой разведки (АР-Р) по соответствующему техническому каналу утечки акустической речевой информации (ТКУРИ).

Особое внимание уделено использованию режима отложенного анализа речевых сообщений (искаженных шумами и помехами), позволяющий значительно повысить качество исходных аудиосигналов. Приведен краткий перечень основных методов шумопонижения, которые могут быть использованы при обработке вторичных сигналов акустоэлектрического канала утечки речевой информации.

Описаны типовые искажения, возникающие в процессе формирования акустоэлектрического канала утечки речевой информации. Рассмотрены характер и степень влияния различных видов искажений на показатели оценки защищенности речевой информации (ЗРИ). Показано, что нелинейные искажения вида «ограничение сверху», наиболее характерные для акустоэлектрического канала утечки, в малой степени снижают разборчивость речи. Наряду со статической моделью речевых сигналов Покровского А.Н., рассмотрена динамическая модель, описываемая фонетической функцией Пирогова А.А. Указаны ограничения статической модели и показан характер влияния динамических признаков на разборчивость речи. Дано объяснение эффектам инвариантности разборчивости речи относительно линейных искажений в канале утечки.

Приведены результаты экспериментальных исследований, в определенной степени, противоречащие некоторым положениям формантной теории разборчивости речи, применяемых для оценки ЗРИ. Определен ряд механизмов повышения помехоустойчивости речевых сообщений, позволяющих выполнять реконструкцию речевых сигналов (РС), искаженных шумами и помехами.

В заключении перечислены предложения по перспективным направлениям совершенствования методов оценки ЗРИ в ТКУРИ.

Ключевые слова: акустическая речевая разведка, акустоэлектрические преобразователи, форманты, фонемы, защита информации, разборчивость речи, речевой сигнал.

Для цитирования. **КОЗЛАЧКОВ, Сергей Б.** et al. НЕКОТОРЫЕ ОСОБЕННОСТИ ФОРМИРОВАНИЯ АКУСТОЭЛЕКТРИЧЕСКОГО КАНАЛА УТЕЧКИ РЕЧЕВОЙ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 60-70, nov. 2017. ISSN 2074-7136. Доступно

на: <https://bit.mephi.ru/index.php/bit/article/view/278>. Дата доступа: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.07.

Sergei B. Kozlachkov[1], Andrew M. Bonch-Bruevich[1], Sergey V. Dvoryankin[2]
Nadezhda V. Vasilevskaya[3], Alexandra L.Selenina[1]
[1]Bauman Moscow State Technical University, 2nd Bauman Street, 5, Moscow, 105005, Russia
e-mail: ksb.perovo@mail.ru, ORCID 0000-0002-7096-6711
e-mail: 123andryb@mail.ru, ORCID 0000-0002-4453-2979
e-mail: so.zz.va@yandex.ru,ORCID 0000-0002-4280-8214
[2]Financial University under the Government of the Russian Federatio (Financial University), LeningradskyProspect, 49, Moscow, 125993, Russia
e-mail: SVDvoryankin@fa.ru, ORCID 0000-0001-6908-0676
[3]FSTEC of Russia, Staraya Basmannaya street, 17, Moscow, 105066, Russia
e-mail: infuzoriavalenoc@yandex.ru, ORCID 0000-0002-0078-8665

Specific features of the formation of an acoustoelectric channel of speech information leakage

DOI: http://dx.doi.org/10.26583/bit.2017.4.07

Abstract. We address the problem of assessing the protection level of the acoustoelectric channel of speech information with respect to leakages associated with specific operation principles of various electromechanical transducers. We analyze the scope of methodological and technical tools for the acoustical speech intelligence (ASI) with respect to corresponding technical channels of leakage of acoustic speech information (TCLSI). Special attention is paid to the regime of timed analysis of speech messages (distorted by noise and interference), allowing one to significantly improve the quality of the original audio signals. We list basic methods of noise reduction that can be used for processing the secondary signals of acoustoelectric leakage channels. We describe typical distortions that occur in the process of the acoustoelectric leakage channel formation. We examine the nature and the degree of the impact of various distortions on the measures of the speech information protection (SIP). We find the effect of the nonlinear distortions of the “upper limit” type (most typical for an acoustoelectric leakage channel) on the speech intelligibility to be in significant. Along with Pokrovsky’s static model of speech signals, we consider a dynamic model based on Pirogov’s phonetic function. The limitations of the static model are discussed, along with revealing the nature of the effect of the dynamic characteristics on speech intelligibility. We explain the effects of invariance with respect to linear distortions in the leakage channel. We perform an experimental study the results of which contradict, to a certain extent, the postulates of the formant theory used to assess the SIP level. We identify a number of mechanisms to improve the noise immunity of voice communications, allowing one to reconstruct speech signals (SS) distorted by noise and interference. We conclude with specifying a number of ways of improving SIP assessment methods in TCLSI.

Keywords: voice acoustic reconnaissance, acoustoelectric transducers, formants, phonemes, information protection, speech intelligibility, speech signal.
For citation. **KOZLACHKOV, Sergei B.** et al. Specific features of the formation of an acoustoelectric channel of speech information leakage. IT Security, [S.l.], v. 24, n. 4, p. 60-70, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/278>. Date accessed: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.07.

Введение

Среди многочисленных технических каналов утечки акустической речевой информации (ТКУРИ) типичным и одним из наиболее сложных в оценке эффективности его защищенности от средств акустической речевой разведки (АР-Р) является акустоэлектрический канал. В первую очередь это связано с тем обстоятельством, что его формирование осуществляется с помощью различных по своей физической природе

принципов преобразования механического (звукового поля) вида энергии в электрический сигнал [1, 2]. Значительное разнообразие типов акустоэлектрических преобразователей: электродинамические; электростатические (конденсаторные, пьезоэлектрические, электретные); электромагнитные; релейные (угольные, транзисторные, оптические и др.) – создает определенные сложности корректного учета условий их функционирования. Другими важными факторами, влияющими на достоверность и точность оценок защищенности речевой информации (ЗРИ) представляются:

- определение возможностей соответствующей модели нарушителя (модель АР-Р);
- оценка характера и степени влияния искажений, вносимых соответствующими преобразователями в канал утечки, на основной показатель оценки защищенности ТКУРИ – разборчивость речи;
- проблема выбора адекватных тестовых сигналов, предназначенных для определения характеристик и измерений значимых параметров опасных сигналов;
- метрологические аспекты при выполнении измерительных процедур.

В рамках данной статьи будут рассмотрены: современные и перспективные способы и методы ведения АР-Р по акустоэлектрическому каналу утечки акустической речевой информации, учитывающие возможности технологий шумопонижения и реконструкции, перехваченных речевых сообщений (РС); а также влияние различного вида искажений, типичных для этого канала.

Модель нарушителя и методы шумопонижения

В отличие от прямого акустического канала утечки, где в т.ч. учитывается вероятность непреднамеренного прослушивания, реализация остальных ТКУРИ принципиально невозможна без использования специальных технических средств АР-Р. Как правило, в состав таких технически сложных и многофункциональных комплексов разведки входят средства звукозаписи (усиления и фиксации) перехваченных сообщений, что позволяет в полной мере реализовать основные достоинства режима отложенного анализа РС [1, 3, 4, 5].

При этом, одним из главных преимуществ такого режима являются не только возможности многократного прослушивания и контекстного анализа с использованием опорных тематических словарей, но и применение достижений современных компьютерных технологий, в т.ч. в области речевых технологий и систем автоматического распознавания речи [4, 5, 6]. Так, многие специалисты отмечали, что с помощью различных методов шумоочистки, точнее методов шумопонижения, коррекции и реконструкции РС можно значительно повысить качество исходных аудиосигналов, что безусловно должно учитываться при оценках ЗРИ [6 - 9].

Применительно к акустоэлектрическому каналу представляется труднореализуемым использование многоканальных синхронных систем шумопонижения, позволяющих с определенными ограничениями повысить предельное соотношение сигнал-шум (*SNR*) в смеси РС с некоррелированными маскирующими шумами [7, 8]. В то же время, наиболее простые и распространенные асинхронные (одноканальные) способы шумопонижения: узкополосные фильтры, медианные фильтры, методы спектрального вычитания, адаптивные фильтры и др. – могут применяться в полном объеме [5, 6, 9].

Отдельного рассмотрения требуют вопросы, связанные с характерными искажениями, возникающими при формировании вторичного сигнала (прошедшего через электроакустический тракт преобразователя), его трансляции по проводным линиям и обработке звукоусилительными каскадами приемного устройства.

Нелинейные искажения

В процессах формирования, преобразования, трансляции и приема исходный аудиосигнал подвергается определенным трансформациям и искажениям, которые могут оказать значительное влияние на его характеристики, в т.ч. на такой показатель ЗРИ,

каким является РР. Оценку характера таких влияний на РР целесообразно проводить не по месту формирования соответствующих искажений, а по их видам и степени влияния: нелинейные искажения, линейные искажения, частотные ограничения.

В общем случае причиной появления нелинейных искажений является нелинейность амплитудной характеристики цепи. По виду нелинейности и характеру изменения сигнала искажения подразделяют на три основных типа: ограничения сверху, центральное ограничение и модуляционные искажения [2, 10]. Основной вклад в образование нелинейных искажений вносят активные элементы электрических цепей с нелинейными вольт-амперными характеристиками.

Как правило, в результате проявлений нелинейных искажений в спектре исходного сигнала появляются новые спектральные составляющие. Мерой нелинейности принято считать коэффициент гармоник. Все искажения незаметны на слух, если уровень продуктов нелинейности ниже абсолютного порога слышимости. В музыкальной акустике принято считать, что порог слуховой заметности нелинейных искажений, измеренных по методу полного коэффициента гармоник (Кг) в диапазоне частот 40Гц…1 кГц, составляет -52 дБ, или 0,25%. Заметность нелинейных искажений существенно снижается за счет эффектов слухового маскирования и других свойств слухового восприятия, повышающих его помехозащищенность.

Инерционные свойства временных характеристик слухового восприятия человека, время адаптации к нелинейным искажениям составляет величину около 10…30 мс, что также позволяет в определенной мере нивелировать негативное влияние нелинейных искажений. Однако необходимо учитывать, что характеры слухового восприятия нелинейных искажений музыкальных и речи имеют существенные различия. Так появление в структуре РС дополнительных спектральных составляющих, обогащающих его спектр, с уровнем коэффициента гармоник до 20…30%, практически не влияет на его разборчивость [11]. Ограничение сверху оказывает минимальное влияние на снижение РР, в силу того, что слуховое восприятие уровня сигнала уже имеет логарифмическую зависимость (log_2x), а это в некоторой степени даже способствует повышению его помехоустойчивости. Даже глубокое клиппирование снижает разборчивость не более чем на 50% [2, 10, 11]. По этим причинам наличие в составе звукоусилительных каскадов систем автоматической регулировки уровня звукозаписи (АРУЗ) с функцией ограничения сигналов высокого уровня не только не снижает РР, а напротив, в определенной степени способствует расширению динамического диапазона фиксируемых сигналов.

Центральное ограничение всегда негативно влияет на РР, поскольку значительно ухудшает восприятие энергии слабых консонантных фонем, составляющих от 30 до 50% разборчивости РС [2].

Наихудшее влияние на РР оказывают нелинейные искажения модуляционного характера, изменяющие не только спектральные, но и временные и динамические параметры РС.

В подавляющем большинстве случаев в акустоэлектрическом канале утечки РИ, в основном, возникают нелинейные искажения вида ограничения сверху, не оказывающие значительного влияния на снижение РР.

Линейные искажения

Наиболее распространенными и наименее значимыми в вышеприведенном перечне искажений являются линейные искажения. Линейные искажения приводят только к изменению соотношения амплитуд и фаз спектральных составляющих сигнала. Такого рода изменения обладают свойством аддитивности: сумма реакций на два воздействия равна реакции на сумму двух воздействий. То есть на выходе линейной цепи не появляются продукты взаимодействия входных сигналов, в результате чего в спектральной структуре РС не образуются новые компоненты.

Основной вклад в образование линейных искажений вносят пассивные элементы электрических цепей с линейными вольт-амперными характеристиками: трансформаторы, конденсаторы, индуктивности, импеданс которых имеет частотную зависимость. Определенную роль оказывают также различные интерференционные волновые эффекты, наиболее характерные для акустических звукоусилительных систем.

В общем случае коэффициент передачи линейного тракта можно представить в виде следующего выражения:

$$K = |K| \bullet e^{j\varphi} \quad (1),$$

где:

$|K|$ – модуль коэффициента передачи, φ – сдвиг фазы, j – комплексная единица.

Зависимость $|K|$ от частоты представляет собой амплитудно-частотную характеристику (АЧХ), а $j\varphi$ – фазочастотную характеристику (ФЧХ).

Наиболее скрупулезно заметность искажений АЧХ исследована в области музыкальной акустики. Так, принято считать, что линейные искажения не будут заметны, если отклонения АЧХ не превышают значений, приведенных в таб.1

Таблица 1 Допустимые значения линейных искажений в акустических системах стереовещания

Диапазон частот	Допустимое отклонение АЧХ	Разбаланс уровней между каналами	Разбаланс фаз между каналами
40…125 Гц	1 дБ	2 дБ	45°
0,125…10 кГц	0,5 дБ	0,5 дБ	30°
10…14 кГц	1 дБ	1,5 дБ	50°
14…15 кГц	2 дБ	2 дБ	90°

В литературе неоднократно отмечалась весьма низкое влияние линейных искажений на восприятие РС [10, 11]. Наихудшее влияние на волновую форму сигнала оказывает нелинейность ФЧХ, которое в определенной степени нивелируется за счет интеграционных процессов механизмов слухового восприятия. Наиболее заметны на слух неравномерности ФЧХ, вызывающие групповое время задержки, которое может достигать существенных значений по мере роста порядка фильтров акустоэлектрического тракта.

В наименьшей степени на РР влияют искажения, вызванные неравномерностью АЧХ передаточного тракта. Так, в музыкальной акустике считается, что пики и провалы АЧХ, ширина которых не превышает 1/8 октавы, на слух практически незаметны. Даже высокие уровни неравномерности АЧХ, формируемые с помощью регулировок эквалайзеров, практически не снижают РР, а только изменяют тембр РС.

Эти факты и другие экспериментальные результаты не укладываются в стандартную формантную теорию РР.

Одним из основных базисов форматной теории является форматный спектр речи, определяемый в виде распределений артикуляционых значений. Принято считать, что интегральный индекс артикуляции речи (R) зависит от вероятности появления формант (k_i) в заданной i-й полосе частот и от уровня эффективного восприятия формант ($P_i(E)$):

$$R = \sum_{i=1}^{N} P_i(E) k_i \quad (2),$$

В соответствии с этим выражением каждое уменьшение уровня эффективного восприятия формант ($P_i(E)$) должно сопровождаться соответствующим снижением артикуляционного индекса и РР, чего на самом деле не происходит [12].

Данный парадокс можно объяснить, прибегнув к иной модели механизма слухового восприятия РС, разработанной А.А. Пироговым [13, 14]. По модели ученого, «каждая фонема отличается главным образом характерным для этой фонемы изменением

спектрального распределения, а не самим спектральным распределением, сопутствующим данной фонеме». Исходя из этих соображений, он ввел понятие «фонетической функции речи», согласно которому фонетические элементы речи целиком определяются законом изменения спектров во времени. В качестве оценки спектральных изменений А.А. Пирогов предложил использовать разность логарифмов интенсивностей двух спектральных разрезов, взятых через интервалы, соответствующие разрешающей способности слуха во времени:

$$P(\omega,t)=\ln\left|\frac{S(\omega,t)}{S(\omega,t-\tau)}\right| \quad (3),$$

где:

$S(\omega, t)$ и $S(\omega, t-\tau)$ – интенсивности спектральных отсчетов РС, взятые через интервал τ, учитывающий разрешающую способность слуха во времени.

Из определения фонетической функции логически вытекает следующий вывод: анализ речи слуховым аппаратом ведется не по изолированным фонемам, а по их звукосочетаниям (дифонам, трифонам – характерным перестройкам речевого аппарата), и именно они являются базовыми фонетическими элементами речи.

Исходя из сказанного, можно сделать вывод о том, что человеческий слух практически инвариантен в отношении амплитудных и фазовых нелинейных искажений, если, конечно, эти искажения не выходят за пределы артикуляторных модуляций и пределов слухового восприятия. Даже полное удаление из РС одной либо двух формант влияет только на тембр звука, однако словесная разборчивость остается высокой.

Данное утверждение можно доказать математически – спектр сигнала, прошедшего через электрический тракт, определяется выражением:

$$Si(\omega,t)=S(\omega,t)Ki \quad (4),$$

где:

$S(\omega,t)$ – спектр входного сигнала, Ki – коэффициент передачи электрического тракта, а $Si(\omega,t)$ – спектр сигнала, прошедшего через электрический тракт.

При допущении, что Ki в период прохождения сигнала не претерпевает нелинейных трансформаций можно выражение (3) представить в следующем виде:

$$P(\omega,t)=\ln\left|\frac{S(\omega,t)Ki}{S(\omega,t-\tau)Ki}\right| \quad (5).$$

Из чего следует фактическая инвариантность фонетической функции А.А. Пирогова (ФФП) относительно АЧХ (Ki) передаточного тракта.

В данной связи применение методов оценки разборчивости речи, основанных на анализе только статических характеристик РС (артикуляционного индекса), представляется недостаточным и неполным. В рамках оценки ЗРИ целесообразно адекватно учитывать и динамические характеристики речи.

В подавляющем большинстве случаев в акустоэлектрическом канале утечки РИ, линейные искажения возникают: в механо-электрических звеньях соответствующих акустоэлектрических преобразователей; в меньшей степени в соединительных проводных линиях (в виду их относительно малой длины); и практически отсутствуют в тракте звукозаписывающей аппаратуры разведывательных комплексов.

В целом можно констатировать относительно незначительный вклад линейных искажений в РР.

Частотные ограничения

Как уже отмечалось выше, наряду с линейными и нелинейными искажениями для акустоэлектрического канала характерными могут являться так же ограничения частотного диапазона РС, записанного техническими разведывательными комплексами. Так, частотный диапазон сигнала может быть ограничен из-за наличия в канале различных

фильтров: ФНЧ, ФВЧ или полосовые фильтры - формируемых различными резонансными цепями. В соответствии с выражением (2), при удалении из состава РС части частотных сегментов его разборчивость должна снижаться [12], однако экспериментально было установлено: при фильтрации РС в полосе частот 100…570 Гц остаточная фразовая РР составляет около 90%, вместо ожидаемых 10…15% [15]. Из чего можно сделать вывод, что данная модель (2) не позволяет в полной мере получить адекватные оценки ЗРИ, поскольку в ней учитываются только статические параметры РС. Между тем, в ряде исследований [13-17] отмечался существенный вклад в РР иных параметров РС, в т.ч. динамических, принципиально не учитываемых Н.Б. Покровским [12].

В общем случае в модели (2) также не всегда справедливо правило аддитивного сложения, что можно доказать в т.ч. экспериментально. Например, если из временной формы РС с регулярным шагом (30 мс) удалить часть сегментов суммарной длительностью около 50%, то можно убедиться, что словесная разборчивость практически не изменилась. Этот эффект можно объяснить влиянием интеграционных процессов слухового восприятия, которые позволяют без особых потерь восстанавливать информацию (сигнальную структуру) пропущенных сегментов речи. Математически это можно пояснить превалирующим положительным влиянием интерполяционных методов над экстраполяционными методами восстановления (реконструкции) сигнала.

Некоторые результаты этого эксперимента, в виде временных и графических сонограмм, приведены на рисунках 1, 2.

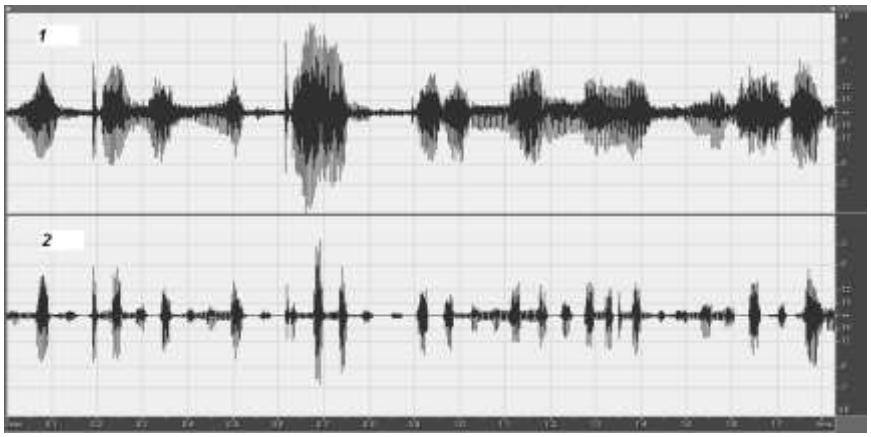


Рисунок 1 - Волновые формы речевого сигнала: 1 – без купюр, 2 – с удаленными сегментами.
(Fig. 1 - The waveform of the speech signal: 1 – uncut, 2 – with remote segments.)

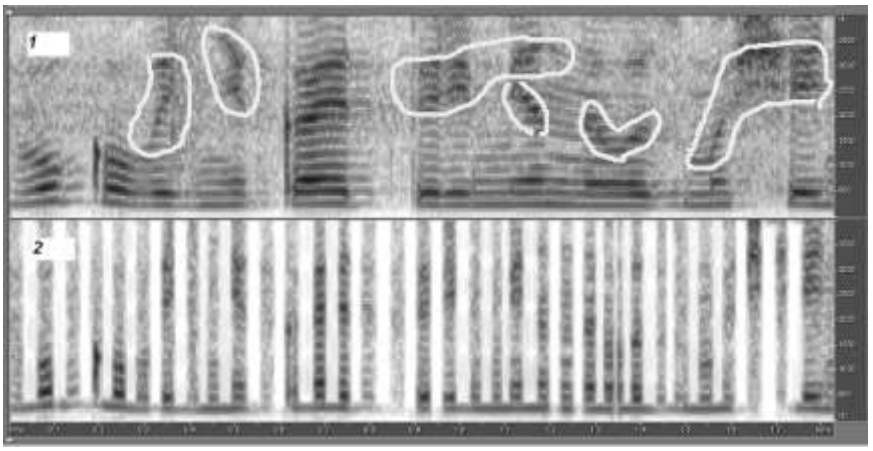


Рисунок 2 - Графические сонограммы речевого сигнала: 1 – без купюр, 2 – с удаленными сегментами. На сонограмме 1 выделены области дифонных переходов.
(Fig. 2 - Graphic of the sonogram of the speech signal: 1 – uncut, 2 – with remote segments. On the sonogram 1 the selected area Divonne transitions.)

Визуально можно убедиться, что на сонограмме 2 (рис. 2) полностью удалены чередующиеся участки сигнала длительностью 30…33 мс, равной или большей длительности оставшихся фрагментов РС.

Таким образом, можно сделать предварительный вывод, что математические интерполяционные методы, сочетающиеся с интеграционными свойствами слухового восприятия, позволяют существенно повысить помехозащищенность РС.

В следующем эксперименте в исходном сигнале были удалены все частоты ниже 100 Гц и выше 570 Гц. Графическая сонограмма такого сигнала приведена на рисунке 3.

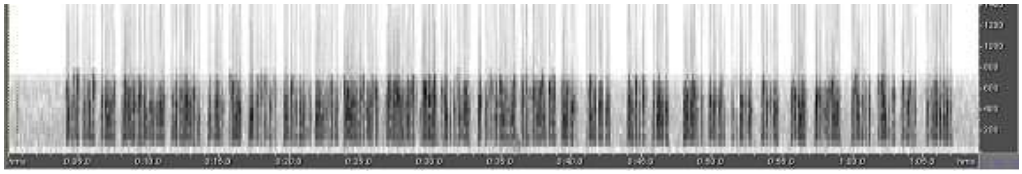


Рисунок 3 - Графическая сонограмма РС ограниченного полосой 100…570 Гц
(Fig. 3 - Graphical sonogram of the speech signal band limited to 100…570 Hz)

Затем такой ограниченный сигнал был дополнительно отфильтрован режекторными фильтрами с частотами: 150 Гц, 300 Гц, 400 Гц и 500 Гц. В результате чего из него были удалены участки суммарной шириной полосы около 200…210 Гц. Волновые формы и графические сонограммы преобразованного РС представлены на рисунках 4, 5. В итоге, остаточная полоса частот этого сигнала составила не более 270 Гц, но фразовая разборчивость снизилась незначительно – до 80…85%.

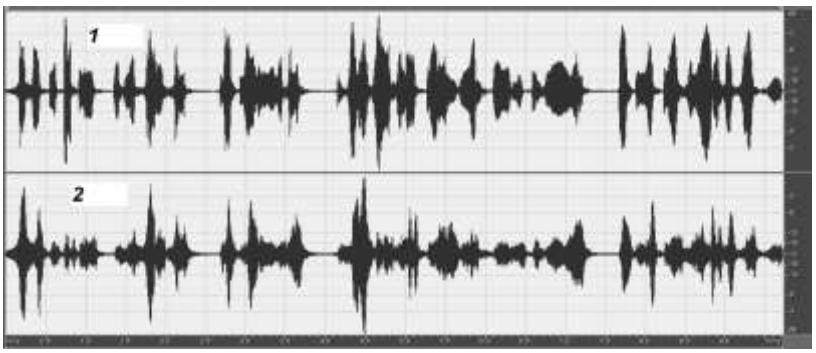


Рисунок 4 - Волновые формы речевого сигнала: 1 – исходный сигнал, отфильтрованный в полосе 100…570 Гц, 2 – отфильтрованный сигнал в полосе 100…570 Гц после применения дополнительных узкополосных фильтров
(Fig. 4 - Wave form of the speech signal: 1 – original signal filtered in the band of 100...570 Hz, 2 – filtered signal in the band of 100…570 Hz after use extra narrowband filters)

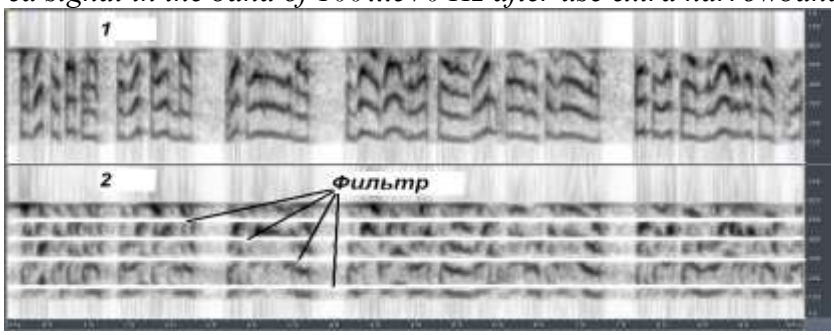


Рисунок 5 - Графические сонограммы речевого сигнала: 1 – исходный сигнал, отфильтрованный в полосе 100…570 Гц, 2 – отфильтрованный сигнал в полосе 100…570 Гц после применения дополнительных узкополосных фильтров
(Fig. 5 - Graphic of the sonogram of the speech signal: 1 – original signal filtered in the band of 570...100 Hz, 2 – filtered signal in the band of 100…570 Hz after use extra narrowband filters)

Усредненные долговременные спектры ограниченного и дополнительно отфильтрованного сигнала показаны на рисунке 6.

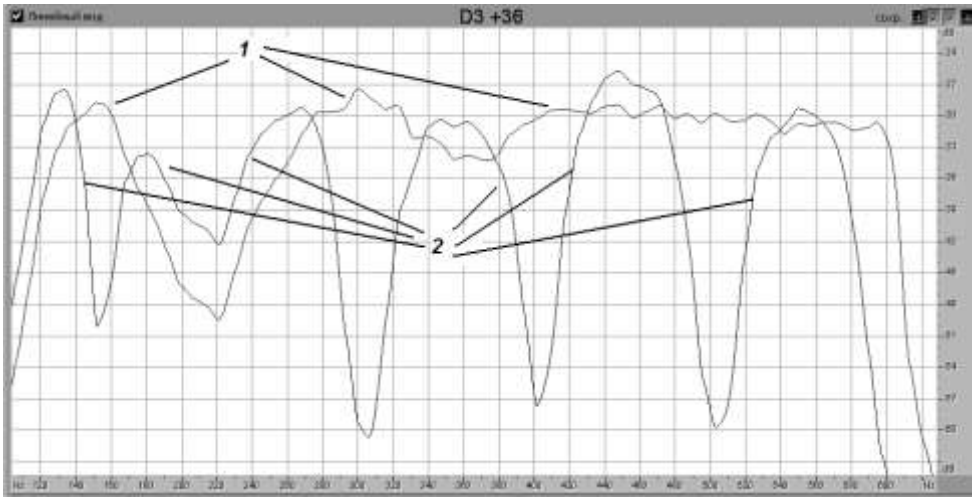


Рисунок 6 - Усредненные долговременные спектры речевого сигнала: 1 – исходный сигнал, отфильтрованный в полосе 100…570 Гц, 2 – отфильтрованный сигнал в полосе 100…570 Гц после применения дополнительных узкополосных фильтров. Удалены участки суммарной полосой частот около 200…210 Гц.

(Fig. 6 - Average long-term spectra of the speech signal: 1 – original signal filtered in the band of 100...570 Hz, 2 – filtered signal in the band of 100…570Hz after use extra narrowband filters. Removed sections with a total bandwidth of about 200… 210Hz)

В этом эксперименте, как и в предыдущем, проявилось влияние интеграционных процессов слухового восприятия и математических интерполяционных методов, нивелирующих частичное ограничение частотного диапазона РС и способствующих повышению его помехоустойчивости.

Отдельного рассмотрения заслуживают динамические параметры РС, тесно связанные с его модуляционными характеристиками. В целом РС формируется путем модуляции гармонической или шумоподобной основы, составляющих вокализованные (гласные и сонорные) и консонантные фонемы соответственно. Сложная структура РС, обусловленная амплитудной, частотной и фазовой модуляцией, позволяет в значительной степени повысить его помехоустойчивость: утрата одних значимых параметров может быть компенсирована за счет других, не подвергшихся чрезмерному искажению.

Другими важными инструментами повышения помехоустойчивости РС являются: эффект коартикуляции, слитное произношение слогов – дифонов и трифонов, объединяющих изолированные фонемы в фонетические элементы речи; а также локусы, позволяющие восстанавливать параметры слабых консонантных фонем по спектральным параметрам примыкающих к ним вокализованных звуков [7, 8].

Крайне важную роль в процессах РР имеют дифонные переходы – выполняющие функцию согласования между консонантными фонемами в пределах одного слова. Именно через дифонные переходы, в определенном понимании, реализуется фонетическая функция А.Н. Пирогова (ФФП). Так на графической сонограмме РС без купюр (позиция 1 на рис.2) выделены области некоторых дифонных переходов. В случае утраты какого-либо участка такого перехода с помощью интерполяционных методов с высокой степенью вероятности, по тренду ФФП и остаточным следам РС можно осуществить восстановление отсутствующего сегмента. Интеграционные процессы слухового восприятия в определенной степени успешно справляются с этой задачей. Однако, необходимо учитывать, что существующие перспективные методы реконструкции РС, искаженных шумами и помехами, могут с большей эффективностью повысить РР. Так, некоторые отечественные программные продукты (Лазурь, Абессин) и другие звуковые

редакторы компании Adobe уже сейчас позволяют восстанавливать графические образы (сонограммы) РС, искаженных шумами и помехами [4-6].

Таким образом, можно сделать определенные выводы относительно возможностей повышения РР для РС, подвергшегося ограничениям частотного диапазона.

Заключение

На основе анализа современных представлений о механизмах повышения помехоустойчивости речевого сигнала и результатов проведенных экспериментальных исследований можно сделать следующие выводы:

1. современные методы и способы ведения АР-Р, основанные на обработке вторичных сигналов в режиме отложенного анализа, позволяют существенно повысить качество исходного РС, искаженного шумами и помехами;
2. действующие методики, не учитывающие в полной мере возможности реконструкции РС, не могут обеспечить необходимой достоверности оценок ЗРИ;
3. формантная теория РР, учитывающая только статические параметры РС, не может далее служить единственной, базовой теоретической основой при разработке новых методик оценок ЗРИ;
4. при разработке новых методик оценки ЗРИ необходимо исследовать и рассмотреть современные модели и описания РС, в т.ч. основанные на взаимодействии динамических и статических параметров, повышающих помехоустойчивость РС.

СПИСОК ЛИТЕРАТУРЫ:

1 Герасименко В.Г., Лаврухин Ю.Н., Тупота В.И. Методы защиты акустической речевой информации от утечки по техническим каналам. М.: РЦИБ Факел, 2008. 256 с.

2 Сапожков М.А. Электроакустика. М.: Связь, 1978. 282 с.

3 Хорев А.А. Техническая защита информации: Учебное пособие для студентов вузов; В 3 т. М.: НПЦ Аналитика, 2008. Т.1. Технические каналы утечки информации. 436 с.

4 Дворянкин С.В., Макаров Ю.К., Хореев А.А. Обоснование критериев эффективности защиты речевой информации от утечки по техническим каналам. Защита информации. INSIDE, 2007. № 2. С. 18–25.

5 Дворянкин С. В., Харченко Л. А., Козлачков С.Б. Оценка защищенности речевой информации с учетом современных технологий шумоочистки. Вопросы защиты информации. 2007. №2 (77). С. 37-40.

6 Дворянкин С.В., Михайлов Д.М., Панфилов Л.А., Козлачков С.Б., Бонч-Бруевич А.М., Насенков И.Г. Интерпретация и контурный анализ спектрограмм звуковых сигналов в процессе их шумоочистки. Проблемы информационной безопасности. Компьютерные системы. 2015. №3. С. 88-99.

7 Козлачков С.Б., Дворянкин С.В., Бонч-Бруевич А.М. Ограничения формантной теории разборчивости речи в приложениях защиты речевой информации. Вопросы кибербезопасности. 2016. №5(18). С. 28-35.

8 Козлачков С.Б., Дворянкин С.В., Бонч-Бруевич А.М. Проблемы и перспективы защиты акустической речевой информации. Специальная техника. 2016. №6. С. 22-29.

9 Скрыль С.В., Бонч-Бруевич А.М., Козлачков С.Б., Никулин С.С. Особенности выделения речевой информации при ее зашумлении с целью защиты. Приборы и системы. Управление, контроль, диагностика. 2014. №2. С. 26-32.

10 Алдошина И.А. Основы психоакустики. Звукорежиссер. 1999. http://www.625-net.ru

11 Журавлев В.Н., Архипова А.Е. Анализ противоречий теорий речеобразования и слуха с позиции идентификации информационных параметров и характеристик речевых сигналов. Информационные технологии и компьютерная инженерия. 2007. №2(9). С. 180-185.

12 Покровский Н. Б. Расчет и измерение разборчивости речи. М.: Связьиздат, 1962. 392 с.

13 Пирогов А.А. Основы Фонетической теории речи. Фонетическая функция как универсальный природный механизм кодирования-декодирования речевой информации любого происхождения. Научный Журнал Русского Физического Общества. 2001. №1-12. С. 15-28.

14 Акбулатов А.Ш., Баронин С.П., Куля В.И., Лейтес Р.Д., Муравьев В.Е., Пирогов А.А., Слуцкер Г.С., Соболев В.Н., Трофимов Ю.К. Вокодерная телефония. Методы и проблемы. М..: Связь, 1974. 536 с.

15 Мишуков А.А. Моделирование процессов управления речевой разборчивостью в многоканальных системах конфиденциальной голосовой связи: диссертация канд. техн. наук: 05.13.18, 05.13.19 Мишуков А.А.. Воронеж. 2012. С. 152

16 Fogerty D., Humes L.E. The role of vowel and consonant fundamental frequency, envelope, and temporal fine structure cues to the intelligibility of words and sentences J. Acoustical Society of America. 2012. 131, № 2. P.

1490–1501.
17 Divenyi P. Perception of complete and incomplete formant transitions in vowels J. Acoustical Society of America. 2009. 126, № 3. P. 1427–1439.

REFERENCES:

[1] Gerasimenko V.G., Lavruhin Ju.N., Tupota V.I. Methods of protection of the acoustic speech information from leakage via technical channels. M.: RCIB Fakel, 2008. P. 256. (In Russian).
[2] Sapozhkov M.A. J Electroacoustics. M.: Svjaz, 1978. P. 282. (In Russian).
[3] Horev A.A. Technical protection of information: Uchebnoe posobie dlja studentov vuzov; V 3 t. M.: NPC Analitika, 2008. T.1. Tekhnicheskie kanaly utechki informacii. P. 436. (In Russian).
[4] Dvorjankin S.V., Makarov Ju.K., Horeev A.A. Substantiation of criteria of efficiency of protection of speech information from leakage via technical channels. Zashhita informacii. INSIDE, 2007. № 2. pp. 18–25. (In Russian).
[5] Dvorjankin S. V., Harchenko L. A., Kozlachkov S.B. Estimation of security of voice information based on modern technology for noise reduction. Voprosy zashhity informacii. 2007. №2 (77). pp. 37-40. (In Russian).
[6] Dvorjankin S.V., Mihajlov D.M., Panfilov L.A., Kozlachkov S.B., Bonch-Bruevich A.M., Nasenkov I.G. Interpretation and contour analysis of spectrograms of sound signals in the process of noise reduction. Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2015. №3. pp. 88-99. (In Russian).
[7] Kozlachkov S.B., Dvorjankin S.V., Bonch-Bruevich A.M. The limitations of the formant theory of speech intelligibility in applications for protection of speech information. Voprosy kiberbezopasnosti. 2016. №5(18). pp. 28-35. (In Russian).
[8] Kozlachkov S.B., Dvorjankin S.V., Bonch-Bruevich A.M. Problems and prospects of protection of the acoustic speech information. Special'naja tehnika. 2016. №6. pp. 22-29. (In Russian).
[9] Skryl' S.V., Bonch-Bruevich A.M., Kozlachkov S.B., Nikulin S.S. Features highlight voice information with its noise masking to protect. Pribory i sistemy. Upravlenie, kontrol', diagnostika. 2014. №2. pp. 26-32. (In Russian).
[10] Aldoshina I.A. Osnovy psihoakustiki. Zvukorezhisser. 1999. http://www.625-net.ru
[11] Zhuravlev V.N., Arhipova A.E. The analysis of contradictions of theories of speech production which lie and hearing from the position identification information of parameters and characteristics of speech signals. Informacionnye tehnologii i komp'juternaja inzhenerija. 2007. №2(9). pp. 180-185. (In Russian).
[12] Pokrovskij N. B. Calculation and measurement of speech intelligibility. M.: Svjazizdat, 1962. P. 392. (In Russian).
[13] Pirogov A.A. Bases of Phonetic theory of speech. Foneticheskaja funkcija kak universal'nyj prirodnyj mehanizm kodirovanija-dekodirovanija rechevoj informacii ljubogo proishozhdenija. Nauchnyj Zhurnal Russkogo Fizicheskogo Obshhestva. 2001. №1-12. pp. 15-28. (In Russian).
[14] Akbulatov A.Sh., Baronin S.P., Kulja V.I., Lejtes R.D., Murav'ev V.E., Pirogov A.A., Slucker G.S., Sobolev V.N., Trofimov Ju.K. Vocoder telephony. Metody i problemy. M..: Svjaz, 1974. P. 536. (In Russian).
[15] Mishukov A.A. A model of speech intelligibility in multi-channel systems, confidential voice: dissertation work of candidate of technical sciences: 05.13.18, 05.13.19 A.A.Mishukov. – Voronezh, 2012. – P. 152. (In Russian).
[16] Fogerty D., Humes L.E. The role of vowel and consonant fundamental frequency, envelope, and temporal fine structure cues to the intelligibility of words and sentences J. Acoustical Society of America. 2012. 131, № 2. P. 1490–1501.
[17] Divenyi P. Perception of complete and incomplete formant transitions in vowels J. Acoustical Society of America. 2009. 126, № 3. P. 1427–1439.

Поступила в редакцию - 19 июня 2017 г. Окончательный вариант – 01 ноября 2017 г.
Received – June 19, 2017. The final version – November 01, 2017.

Роман А. Устинов
Финансовый университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский пр-т, 49, г. Москва, 125993, Россия
e-mail: public-ura@yandex.ru, ORCID 0000-0002-8454-9951

ОСОБЕННОСТИ СОВРЕМЕННЫХ СИСТЕМ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2017.4.08

Аннотация. На сегодняшний день речевые технологии являются одним из самых активно развивающихся секторов в мировой экономике. В связи с чем, вопросы обеспечения безопасности речевой информации (РИ) остаются весьма актуальными. В рамках данной работы рассмотрены системы защиты РИ для современной модели связи. Такая модель является мультимодальной и многопотоковой и подразумевает наличие большого числа абонентов, которые имеют возможность использовать несколько линий связи для организации своего взаимодействия. С учетом этого проведен детальный анализ угроз конфиденциальности, целостности и доступности РИ. Рассмотрены существующие методы противодействия данным угрозам. Показано, что имеющиеся методы не обеспечивают безопасность речевых сообщений (РС) в полной мере и существует ряд новых угроз в области обеспечения целостности и доступности РИ, для которых на текущий момент решения отсутствуют или находятся на стадии разработки. Предложены собственные подходы для противодействия таким угрозам. Для обеспечения целостности РС наиболее перспективными являются методы стеганографии, в частности применение аудиомаркеров позволит однозначно аутентифицировать личность говорящего на протяжении всего сеанса связи. Для противодействия угрозам доступности РИ в части, касающейся пропускной способности канала связи и ограниченных объемов хранилищ данных РС, необходимы усовершенствование существующих и разработка новых адаптивных алгоритмов сжатия речи. При чем такие алгоритмы должны сохранять заданный уровень речевой разборчивости.

Ключевые слова: защита речевой информации, угрозы информационной безопасности, речевая разборчивость, аудиомаркер, адаптивное алгоритмы сжатия речи

Для цитирования. **УСТИНОВ, Роман А.** ОСОБЕННОСТИ СОВРЕМЕННЫХ СИСТЕМ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 73-81, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/279>. Дата доступа: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.08.

***Благодарности:** Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета 2017 года.

Roman A. Ustinov
Financial University under Government of the Russian Federation (Financial University),
Leningradsky Prospekt, 49, Moscow, 125993, Russia
e-mail: public-ura@yandex.ru, ORCID 0000-0002-8454-9951

Specific features of modern voice protection systems

DOI: http://dx.doi.org/10.26583/bit.2017.4.08

Abstract. Nowadays, speech technologies are among the most vibrant sectors of the world's economy. Of high importance is the problem of ensuring the security of speech information (SI). Here we discuss SI protection systems within a modern communication model. The model is multimodal, multithreaded, and implies a large number of subscribers interacting via several communication lines. With this in mind, we perform a detailed analysis of threats to the confidentiality, integrity and accessibility of SI. Existing methods of counteraction against these threats are discussed, and shown to be insufficient to ensure the safety of voice messages (VM) in full. Mean while, there are new threats to the integrity and accessibility of SI, the solutions for

which are either do not exist, or only being developed. We propose our original approach to counter these threats. Steganography methods are the most promising for ensuring the integrity of the VM. In particular, using audiomarkers allows one to reliably trace speaker'sidentity throughout the entire communication session. In order to counter the threats to SI availability due to the capacity of the communication channel and the limited volumes of VM data storage, it is necessary to improve existing adaptive speech compression algorithms, along with developing new ones. Furthermore, such algorithms must keep the specified level of speech intelligibility.
Keywords: protection of speech information, threats to information security, speech intelligibility, audiomarker, adaptive compression algorithms
For citation. **USTINOV, Roman A.** Specific features of modern voice protection systems. IT Security, [S.l.], v. 24, n. 4, p. 73-81, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/279>. Date accessed: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.08.
***Acknowledgements:** The article is prepared on the basis of the results of studies carried out at the expense of budget funds under the state task of the Financial University of 2017.

Введение

Несмотря на высокие темпы развития телекоммуникационных технологий, человеческая речь продолжает оставаться одним из самых популярных способов общения между людьми. Так, аналитики Forbes отмечают, что рынок речевых технологий является одним из самых динамично развивающихся секторов экономики в мире. По их прогнозам, к 2022 году он увеличится до 12 млрд, в качестве основной движущей силы отмечаются постоянно растущие потребности в речевых технологиях в области безопасности, телекоммуникациях, колл-центрах и B2C (Business-to-consumer) секторе [1].

Такое положение дел обусловлено тем, что речь является уникальным психолингвистическим процессом. Она обладает рядом признаков, присущим только ей: эффект присутствия, эмоциональная окраска, информационная избыточность и т.п.[2] Таким образом, задача защиты речевой (акустической) информации (РИ) на сегодняшний момент не потеряла своей актуальности, а в связи с постоянно развивающимися технологиями речевой обработки, а также средствами акустической (речевой) разведки приобретает все большее значение[3].

Модель многопотоковой мультимодальной системы связи

На современном этапе развития систем связи, традиционная модель голосовой связи, представленная на рисунке 1, значительно изменилась.

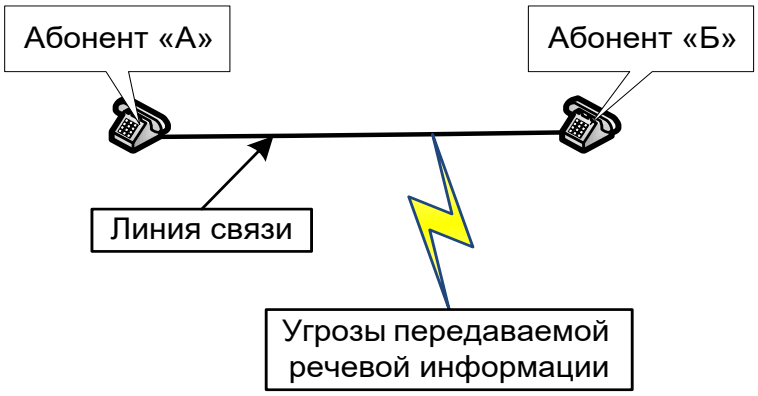


Рисунок 1 - Традиционная модель связи абонентов
(Fig. 1 - Traditional model of communication subscribers)

В настоящее время актуальная модель связи абонентов представляет собой мультимодальную многопотоковую систему, в которой участвует много абонентов и

может быть задействовано несколько линий связи. Такая модель представлена на рисунке 2.

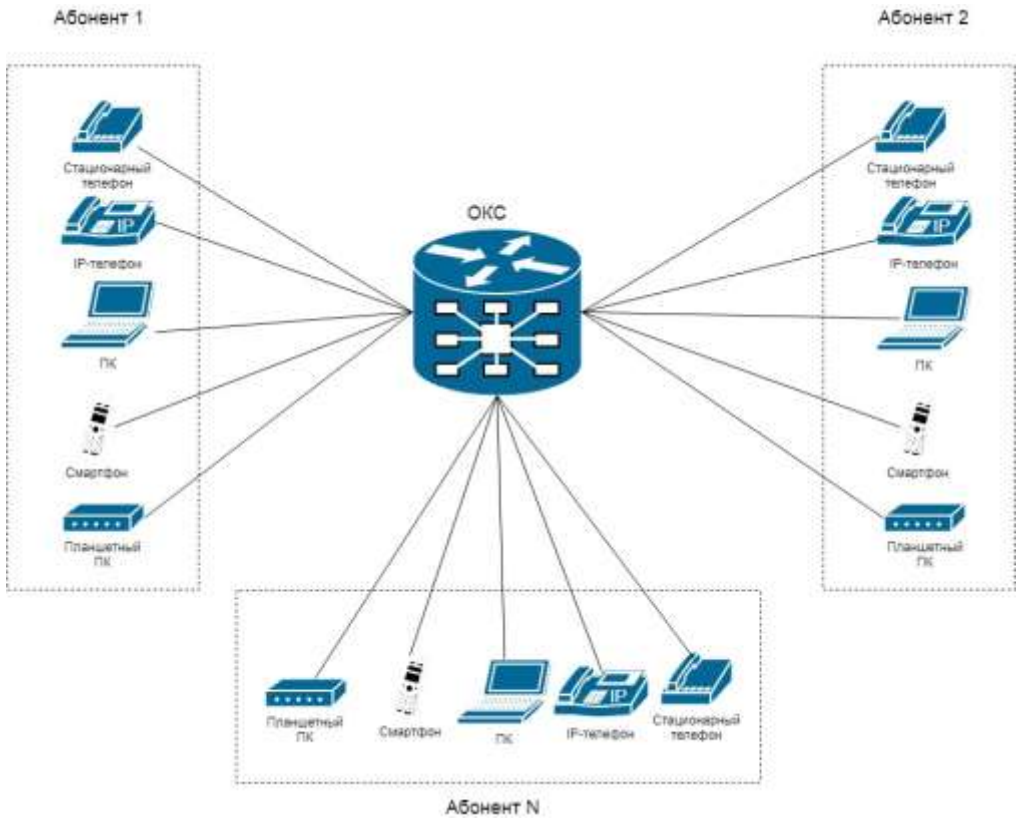


Рисунок 2 - Актуальная модель связи абонентов (много абонентов - много линий связи)

(Fig. 2 - Current model of subscribers (a lot of subscribers - a lot of lines))

Актуальные угрозы речевой информации при ее передаче по общедоступным каналам связи

Как и для любого другого вида информации защищенность РИ на практике рассматривается как совокупность трех основополагающих понятий: конфиденциальность, целостность, доступность [4].

Основными элементами описания угроз информационной безопасности являются:

- источник угрозы;
- среда распространения информативного сигнала;
- носитель защищаемой информации.

В качестве источников угроз безопасности РИ можно рассматривать злоумышленников (физические лица, юридические лица, криминальные, террористические группировки, разведывательные службы государств), осуществляющих перехват (съем) информации с использованием технических средств ее регистрации.

Среда распространения информативного сигнала (РИ) - это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником.

Носителем защищаемой РИ являются акустические (речевые) сигналы.

С учетом вышеизложенного, рассмотрим современные угрозы РИ.

Угрозы конфиденциальности

Угрозы конфиденциальности направлены на получение несанкционированного доступа к РИ и напрямую связаны с угрозами свойственными каналам связи и аппаратно-программным средствам передачи голосовой информации. Это обусловлено тем, что во время передачи голосовой (звуковой) информации, она является наиболее доступной и менее защищённой для нарушителя, не обладающего специальными дорогими устройствами акустической (речевой) разведки на уровне специальных служб, но обладающего знаниями обо всех технологических процессах обработки такой информации.

Определим основные угрозы конфиденциальности РИ:

- применение подслушивающих устройств и видеосъемка с аудио сопровождением;
- обнаружение и анализ побочных электромагнитных излучений и наводок;
- перехват данных, передаваемых по каналам связи, и их последующий анализ для определения протоколов обмена, правил установления сеансов связи и авторизационных параметров пользователя с целью получения доступа к защищаемой РИ;
- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, MAC-адрес, адрес в системе связи, аппаратный блок кодирования;
- внедрение аппаратных и/или программных "закладок", вирусного программного обеспечения, позволяющих преодолевать систему зашиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи защищаемой информации.

Угрозы целостности

В общем смысле целостность защищаемой информации, во-первых, обеспечивает неизменность данных на предполагаемом этапе жизненного цикла обработки информации со стороны нелегитимных пользователей (статистическая целостность), а во-вторых, гарантирует то, что информация внутренне непротиворечива и отражает реальное положение вещей (динамическая целостность)[4].

К угрозам статической целостности относятся[5]:

- незаконное изменение информации, фальсификация информации (дезинформация);
- фальсификация автора сообщения, то есть нарушение аутентичности - гарантии того, что источником информации является именно тот, субъект, который заявлен как ее автор;
- нарушение аппелированности сообщения, то есть гарантия авторства сообщения - возможность доказать, что автором сообщения является именно заявленный субъект.

Угрозами динамической целостности является нарушение атомарности транзакций, внедрение нелегальных пакетов в информационный поток и т.д.

Угрозы доступности

Угрозы доступности РИ, в свою очередь, также обусловлены указанными особенностями построения каналов голосовой связи, однако дополнительно включают в себя вопросы помехозащищенности и пропускной способности.

К подобного рода угрозам относятся [6]:

- физическое воздействие на вычислительную систему (ВС) или отдельные ее части с целью вывода ВС из строя, уничтожения, нарушения регламентированного порядка функционирования;

- физическое воздействие на подсистемы обеспечения функционирования ВС (электропитания, охлаждения и т.п.);
- изменение режимов работы устройств или программ;
- различные методы ведения радиоэлектронной борьбы и/или информационного воздействия (создание активных радиопомех на частотах работы устройств системы и т.п.);
- внедрение аппаратных и/или программных "закладок", вирусного программного обеспечения с целью дезорганизации функционирования ВС;
- угрозы типа отказ в обслуживании (Denial of Service - DoS) - атака на ВС с целью довести её до отказа, то есть создание таких условий, при которых легитимные пользователи системы не могут получить доступ к предоставляемым ВС ресурсам, либо этот доступ затруднён.

Методы обеспечения безопасности речевой информации

Оборонительный аспект создаваемых с помощью информационных технологий средств обеспечения информационной безопасности РИ в открытых, общедоступных каналах связи (ОКС), требует от разработчика комплексного подхода к решению проблемы защиты речевых сообщений (РС). То есть построение систем защиты РИ должно проводиться с учетом всех возможных угроз, и исходя из предположения, что злоумышленник (ЗЛ) обладает всем необходимым арсеналом знаний и технического оборудования для осуществления несанкционированного доступа к РИ в ОКС.

На рисунке 3 представлены методы защиты РИ от угроз конфиденциальности, целостности и доступности. Рассмотрим каждый из представленных методов более подробно.

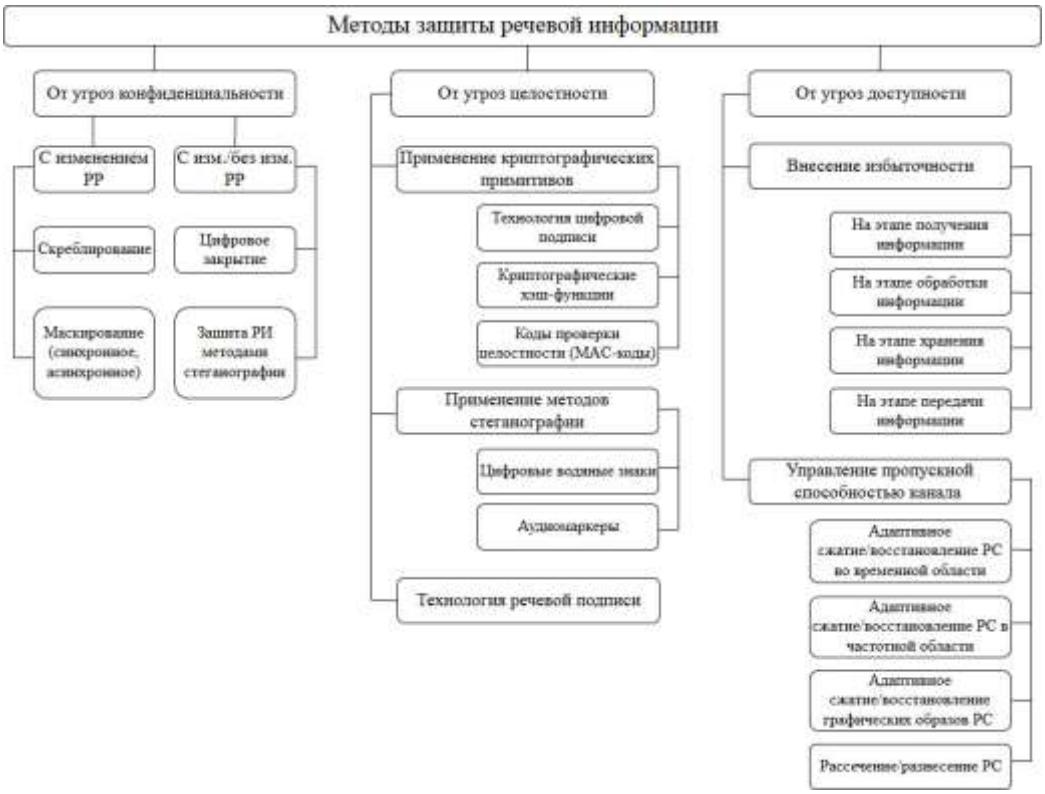


Рисунок 3 - Методы защиты речевой информации
(Fig. 3 - Methods of protection of speech information)

Методы защиты речевой информации от угроз нарушения конфиденциальности

На сегодняшний день существует большое количество различных методов, обеспечивающих безопасность РИ при ее передаче по ОКС. Данные методы основываются на преобразованиях речевых сигналов, изменяющих характеристики РС, затрудняя их разборчивость и узнаваемость для ЗЛ.

Основным показателем защищенности РИ от угроз конфиденциальности является речевая разборчивость (РР) - отношение количества принятых слушателем (артикулянтом) элементов речи к общему количество переданных элементов речи. В зависимости от способов изменения РР различают методы защиты РИ с изменением или без изменения РР.

К методам с изменением РР относятся: *маскирование, аналоговое скремблирование (преобразование)*.

Под *маскированием* понимается синтез спектра маскированного речевого сигнала, путем внесения амплитудно-частотного искажения, обеспечивающий максимальную скрытность передачи сигнала при наилучшем качестве восстановленной речи. Различают синхронное (требуется наличие блока (схемы) синхронизации) и асинхронное маскирование РИ.

Под *скремблированием* понимается изменение характеристик исходного речевого сигнала таким образом, чтобы преобразованный (защищенный) сигнал был неразборчив и неузнаваем, но занимал такую же полосу частот спектра, как и исходный открытый речевой сигнал [7, 8].

Цифровое закрытие РИ и защита РИ методами стеганографии могут применяться как методы с изменением, так и без изменения РР. Это обусловлено тем, что использование указанных методов условно можно разбить на два эта.

В случае цифрового закрытия - это преобразование речевого сигнала (без изменения или с изменением РР) в цифровую форму и применение криптографических алгоритмов.

В случае использования стеганографических методов - это предварительная обработка речевого сигнала (в цифровой или аналоговой форме с изменением/без изменения РР) и последующее внедрение в стегоконтейнер. Стоит отметить, что данный метод позволяет обеспечить не только конфиденциальность передаваемого РС, но и скрыть сам факт передачи. Среди наиболее распространенных вариантов использования стеганографии для обеспечения безопасности РИ могут использоваться[5]:

- скрытная передача РИ в информационных сообщениях иного вида (видео, изображение, текст);
- скрытная передача РИ в другом речевом сигнале.

Методы защиты речевой информации от угроз нарушения целостности

На практике задачи обеспечения целостности информации решаются путем применения различных криптографических примитивов[4]:

- технология цифровой подписи;
- криптографические хэш-функции;
- коды проверки подлинности (MAC-коды).

В дополнение к указанным способам защиты РС от угроз целостности могут применяться[9, 10]:

- стеганографические методы (выявление признаков незаконного копирования аудио и видеозаписей может осуществляться по цифровым водяным знакам и др.);
- технология речевой подписи (повышение защищенности документооборота).

Однако для РИ появляются новые угрозы нарушения целостности, обусловленные интенсивным развитием речевых технологий и методов повышения качества обработки речевого сигнала.

Так, в августе 2017 года на ежегодной конференции и выставке в области компьютерной графики и интерактивных технологий SIGGRAPH 2017 специалистами из Вашингтонского университета были продемонстрированы возможности нейросетевых технологий по синтезу реалистичного видео с использованием аудиозаписей. Им удалось сформировать высокореалистичное фейковое видео с Бараком Обамой. Для этого потребовалось всего лишь 14 часов, в течении которых нейросеть обучалась правильной синхронизации движений губ и речевого потока на образцах выступлений бывшего президента США, находящихся в свободном доступе.

Еще одним ярким примером может служить возросшее число случаев телефонных "пранков" и мошенничеств, когда при помощи технологий синтеза человеческой речи ЗЛ выдают себя за других людей.

Таким образом, возникает задача подтверждения подлинности источника РС на всем интервале ведения разговора, в том числе и при организации видеоконференцсвязи. Одним из решений данной проблемы может служить внедрение аудиомаркеров (некоторый аналог цифровых водяных знаков) в речевой поток для однозначной аутентификации личности говорящего [11, 12].

Методы защиты речевой информации от угроз нарушения доступности

Угрозы доступности РИ обусловлены уязвимостями каналов связи, поэтому нейтрализация указанных угроз достигается путем введения той или иной избыточности. На текущий момент существует достаточное количество апробированных решений в этой области, некоторые из которых отражены на рисунке 4 [4].

Рисунок 4 - Структура системы защиты от угроз нарушения доступности (Fig. 4 - The structure of the system of protection against threats of violation of availability)

Но несмотря на широкий спектр существующих методов противодействия угрозам нарушения доступности, для систем защиты РИ есть ряд специфических задач, в области которых решения отсутствуют, либо находятся на стадии разработки.

Весьма актуальной представляется задача накопления и хранения архивов РИ, возникшая в результате принятия 6 июля 2016 г. федеральных законов № 374-ФЗ и

№ 375-ФЗ ("пакет Яровой"), которые в том числе обязывают операторов связи хранить звонки абонентов за определенный период.

Кроме того, существует традиционная задача управления пропускной способностью канала связи в условиях активного информационно-технического воздействия ЗЛ.

Решение данных задач подразумевает разработку новых и усовершенствование существующих адаптивных методов сжатия РИ с сохранением максимального уровня РР в условиях ограниченного объема хранилища данных или в условиях низкой пропускной способности канала связи [13, 14].

Заключение

Несмотря на бурное развитие информационных технологий, РИ до сих пор занимает значительную часть в общем объеме предаваемой информации даже в условиях изменившейся модели связи абонентов. С учетом этого изменился и приоритет традиционных угроз безопасности РИ, появились новые угрозы.

Можно считать, что наиболее защищенной РИ остается от угроз нарушения конфиденциальности. Такое положение дел обусловлено тем, что традиционно конфиденциальность считается наиболее значимым свойством безопасности информации. Для обеспечения защиты РС от несанкционированного доступа разработан и применяется широкий спектр как программных, так и программно-аппаратных средств защиты, основанных на реализации одного или комбинации нескольких методов защиты РИ: маскирование, скремблирование, цифровое закрытие или стеганография.

Однако с учетом постоянно развивающихся речевых технологий растет и значимость обеспечения безопасности РИ от угроз нарушения целостности и доступности. Данные вопросы требуют более внимательного и комплексного подхода для своего решения.

Для защиты РС от угроз нарушения целостности весьма перспективными видятся методы стеганографии. Например, для подтверждения личности участников переговоров в ОКС можно использовать технологию встраивания аудиомаркеров в РС.

Для противодействия угрозам доступности РИнеобходима разработка и исследование новых методов адаптивного сжатия речи с сохранением заданного уровня РР и повышения пропускной способности ОКС, в том числе на основе образного анализа-синтеза речевого сигнала.

СПИСОК ЛИТЕРАТУРЫ:

1 Федорин М. Они нас слышат: куда развиваются речевые технологии? "Forbes Russia". URL: http://www.forbes.ru/tekhnologii/331035-oni-nas-slyshat-kuda-razvivayutsya-rechevye-tekhnologii (дата обращения: 11.09.2017).

2 Устинов Р.А. Проблема обеспечения информационной безопасности при передаче аудиовизуальных данных по общедоступным каналам связи. Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2011. № 3. URL: http://technomag.bmstu.ru/doc/168981.html (дата обращения: 13.09.2017).

3 Дворянкин С.В., Козлачков С.Б., Харченко Л.А. Оценка защищенности речевой информации с учетом современных технологий шумоочистки. Вопросы защиты информации № 2. 2007. с. 18-21.

4 Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. URL: http://ss-sks.narod.ru/is/lit01.pdf (дата обращения: 15.09.2017).

5 Пузыренко А.Ю, Конахович Г.Ф. Компьютерная стеганография. Теория и практика. К.: "МК-Пресс", 2006. 288 с.

6 Park P.VoIP Threat Taxonomy Cisco Press. URL: http://www.ciscopress.com/articles/article.asp?p=1245881 (дата обращения: 21.09.2017).

7 Дворянкин С.В. Компьютерные технологии защиты речевых сообщений в каналах электросвязи. Учебное пособие. М.: РИО МТУСИ, 1999. 52 с.

8 Дворянкин С.В., Мишуков А.А. Маскирование речевой информации: перспективные методы и средства. "Спецтехника и связь" № 3. 2009. с. 46-51.

9 Дворянкин С.В., Минаев В.А. Возможности скрытой передачи информации по общедоступным каналам речевой связи. Тезисы докладов 7-й Международной конференции "Информатизация правоохранительных систем". М: Академия управления МВД РФ, 1997. ч. 2. с. 78-79.

10 Дворянкин С.В., Минаев В.А. Технология речевой подписи. Открытые системы. - М.1997. № 5 (25). с. 68-71.
11 Дворянкин С.В., Дворянкин Н.С. Способ установления подлинности речевых сообщений, передаваемых по каналам сотовой связи. Спецтехника и связь. 2015. № 4. с. 32-39.
12 Scheips D. Voice recognition - benefits and challenges of this biometric application for access control SourceSecurity.com. URL: https://www.sourcesecurity.com/news/articles/co-3108-ga.4100.html (дата обращения: 21.09.2017).
13 Sun L., Mkwawa IH., Jammeh E., Ifeachor E. Speech Compression Springer International Publishing AG. URL: https://link.springer.com/chapter/10.1007%2F978-1-4471-4905-7_2 (дата обращения: 21.09.2017).
14 Дворянкин С.В., Калужин Р.В. Адаптивное сжатие аудиоинформации в системах защиты и обработки. "Системы безопасности", № 6(48), 2002. с. 94-96.

REFERENCES:

[1] Fedorin M. Oni nas slyishat: kuda razvivayutsya rechevyie tehnologii ? "Forbes Russia". URL: http://www.forbes.ru/tekhnologii/331035-oni-nas-slyshat-kuda-razvivayutsya-rechevye-tekhnologii (accessed: 11.09.2017).
[2] Ustinov R.A. Problema obespecheniya informatsionnoy bezopasnosti pri peredache audiovizualnyih dannyih po obschedostupnyim kanalam svyazi. Nauka i obrazovanie. MGTU im. N.E. Baumana. Elektron. zhurn. 2011. no 3 URL: http://technomag.bmstu.ru/doc/168981.html (accessed: 13.09.2017).
[3] Dvoryankin S.V., Kozlachkov S.B., Harchenko L.A. Estimation of security of voice information with the modern technology of noise-cancellation. Voprosyi zaschityi informatsii no 2. 2007.pp. 18-21. (In Russian).
[4] Tsirlov V.L. Osnovyi informatsionnoy bezopasnosti avtomatizirovannyih sistem. Kratkiy kurs. URL: http://ss-sks.narod.ru/is/lit01.pdf (accessed: 15.09.2017).
[5] Puzyirenko A.Yu, Konahovich G.F. Computer steganography. Teoriya i praktika. K.: "MK-Press", 2006. 288 p.
[6] Park P. VoIP Threat Taxonomy Cisco Press. URL: http://www.ciscopress.com/articles/article.asp?p=1245881 (accessed 21.09.2017).
[7] Dvoryankin S.V. Computer protection technology voice messages in telecommunication channels. Uchebnoe posobie. M.: RIO MTUSI, 1999. 52 p.(In Russian).
[8] Dvoryankin S.V., Mishukov A.A. Masking of speech information: advanced methods and tools. "Spetstehnika i svyaz" no 3. 2009. pp. 46-51 (In Russian).
[9] Dvoryankin S.V., Minaev V.A. The possibility of hidden transmission of information through public channels voice communications. Tezisyi dokladov 7-y Mezhdunarodnoy konferentsii "Informatizatsiya pravoohranitelnyih sistem". M: Akademiya upravleniya MVD RF, 1997. vol. 2. pp. 78-79. (In Russian).
[10] Dvoryankin S.V., Minaev V.A. Technology voice signature. Otkryityie sistemyi. - M.1997. no 5 (25). pp. 68-71. (In Russian).
[11] Dvoryankin S.V., Dvoryankin N.S. The method of establishing the authenticity of voice messages transmitted over cellular channels. Spetstehnika i svyaz. 2015. no 4. pp. 32-39. (In Russian).
[12] Scheips D. Voice recognition - benefits and challenges of this biometric application for access control SourceSecurity.com. URL: https://www.sourcesecurity.com/news/articles/co-3108-ga.4100.html (accessed: 21.09.2017).
[13] Sun L., Mkwawa IH., Jammeh E., Ifeachor E. Speech Compression Springer International Publishing AG. URL: https://link.springer.com/chapter/10.1007%2F978-1-4471-4905-7_2 (accessed: 21.09.2017).
[14] Dvoryankin S.V., Kaluzhin R.V. Adaptive compression of audio in security systems and processing. "Sistemyi bezopasnosti", no. 6(48), 2002. pp. 94-96.

Поступила в редакцию - 19 июня 2017 г. Окончательный вариант – 01 ноября 2017 г.
Received – June 19, 2017. The final version – November 01, 2017.

Вячеслав М. Барбашов[1], Олег А. Калашников[2]
[1]Национальный исследовательский ядерный университет «МИФИ», 115409, Москва, Каширское шоссе, 31, Россия
e-mail: VMBarbashov@mephi.ru,ORCID 0000-0001-7136-415X
[2]АО«ЭНПОСПЭЛС»
115409, Москва, Каширское шоссе, 31, Россия
e-mail: oakal@spels.ru, ORCID 0000-0002-9473-9900

ФУНКЦИОНАЛЬНО-ЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДОЗОВЫХ РАДИАЦИОННЫХОТКАЗОВСФ-БЛОКОВ СИСТЕМ НА КРИСТАЛЛЕ

DOI: http://dx.doi.org/10.26583/bit.2017.4.09

Аннотация: Рассмотрена методика функционально-логического моделирования дозовых радиационных отказов систем на кристалле, основанная на методе критериальных функций принадлежности. Проведен анализ возможностей данного подхода для определения работоспособности СФ-блоков и влияния на нее режимов функционирования.Исследованы особенности применения методики для моделирования дозовых радиационных отказов различных типов СФ-блоков: логических элементов, блоков и ячеек памяти, процессоров. Приведены примеры построения критериальных функций принадлежности и функций работоспособности этих СФ-блоков по различным критическим параметрам, характеризующим их отказы. Показано, что при моделировании дозовых отказов необходимо учитывать влияние режима функционирования в процессе облучения на параметры моделей.Предложенная методика позволяет повысить достоверность оценки показателей радиационной стойкости СнК, в том числе с целью решения задач обеспечения информационной безопасности радиоэлектронной аппаратуры.

Ключевые слова: СнК, дозовые радиационные отказы, функционально-логическое моделирование.

Для цитирования. **БАРБАШОВ, Вячеслав М.; КАЛАШНИКОВ, Олег А.** ФУНКЦИОНАЛЬНО-ЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДОЗОВЫХ РАДИАЦИОННЫХ ОТКАЗОВ СФ-БЛОКОВ СИСТЕМ НА КРИСТАЛЛЕ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 80-86, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/283>. Дата доступа: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.09.

VyacheslavM.Barbashov[1], OlegA.Kalashnikov[2]
[1]National Research Nuclear University MEPHI
Kashirskoeshosse, 31, Moscow, 115409, Russia
e-mail: VMBarbashov@mephi.ru, ORCID 0000-0001-7136-415X
[2] JSC "ENGOs SPELS",
Kashirskoeshosse, 31, Moscow, 115409, Russia
e-mail: oakal@spels.ru, ORCID 0000-0002-9473-9900

Functional-logic simulation of IP-blocks dose functional failures

DOI: http://dx.doi.org/10.26583/bit.2017.4.09

Abstract. The technique of functional-logical simulation of System-on-Chip (SoC) total dose radiation failures is presented based on fuzzy logic sets theory. An analysis of the capabilities of this approach for IP-blocks radiation behavior is carried out along with the analysis of operating modes under irradiation influence on IP-blocks radiation behavior. The following elements of this technique application for simulation of dose radiation failures of various types of IP-units are studied: logical elements, memory units and cells, processors. Examples of criterial membership functions and operability functions construction are given for these IP-units and for various critical parameters characterizing their failures. It is shown that when modeling total dose failures it is necessary to take into account the influence of the functional mode on the

model parameters. The technique proposed allows improving the reliability of the SoC radiation hardness estimation, also for the purpose of solving the problems of information security of electronic devices.

Keywords: SoC, total dose failures, functional-logical simulation.

For citation. **BARBASHOV, Vyacheslav M.; KALASHNIKOV, Oleg A.** Functional-logic simulation of IP-blocks dose functional failures. IT Security, [S.l.], v. 24, n. 4, p. 80-86, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/283>. Date accessed: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.09.

Повышение сложности и функциональной насыщенности радиоэлектронных систем и комплексов невозможно без внедрения современной электронно-компонентной базы (ЭКБ), такой как «системы на кристалле» (СнК). Их применение радикально улучшает массогабаритные показатели, потребляемую мощность, быстродействие и функциональные возможности радиоэлектронной аппаратуры (РЭА). Применение СнК на основе сложно-функциональных блоков (СФ-блоков) дает разработчику РЭА широкие возможности по гибкому управлению системными ресурсами, оперативному созданию аппаратурно и системно ориентированных СнК [1].

Современные радиоэлектронные системы и комплексы специальной техники в составе бортовых атомно-энергетических и ядерных комплексов, космических аппаратов, авиационных систем должны функционировать в жестких условиях эксплуатации, подвергаясь различным видам радиационных воздействий. Для решения задач по обеспечению радиационной стойкости таких систем необходимо определять и контролировать стойкость используемой ЭКБ, в том числе СнК, как на этапе производства, так и на стадии выбора ЭКБ при проектировании РЭА[2-4].

Возможности экспериментальной оценки радиационной стойкостисверхбольших интегральных схем (СБИС) класса СнК ограничены, т.к., с одной стороны,такая оценка сопряжена со значительными временными и трудозатратамипо подготовке и проведению радиационных испытаний, а с другой – не всегда дает достоверный результат в силу значительного разнообразия функциональных узлов в составе СнК и режимов их работы [5]. Альтернативой является расчетный подход к оценке стойкости. В [6,7]предложен метод функционально-логического моделирования дозовых радиационных отказов цифровых интегральных схем, основанный на математическом аппарате нечеткой логики. Рассмотрим возможности данного подхода для определения работоспособности СФ-блоков и влияния на нее режимов функционирования.

Для простых логических элементов, радиационный отказ которых проявляется как деградация выходных напряжений логических "0" и "1", порог работоспособности определяется по зависимостям этих напряжений от уровня воздействия (поглощенной дозы). На рисунке 1 показана измеренная зависимость $U_{вых}^{1}(D)$ КМОП инвертора 564ЛН2. Аналогично выглядят зависимости $U_{вых}^{1}(D)$ и для других логических КМОП элементов (И-НЕ, ИЛИ-НЕ). Их резкий характер позволяет легко определить порог работоспособности [8].

Такой же подход нередко применим и для СФ-блоков. На рисунке 2 показаны измеренные зависимости напряжений выходных логических уровней "0" и "1" СФ-блока постоянного запоминающего устройства с электрическим стиранием (ЭСППЗУ) от поглощенной дозы[9]. Показаны также рассчитанные по этим зависимостям функции принадлежности, причем в качестве критериев выбраны указанные в спецификации предельно допустимые значения (1,2 В для логической "1" и 0,2 В для логического "0" при $E_{пит}$ = 2,5 В).

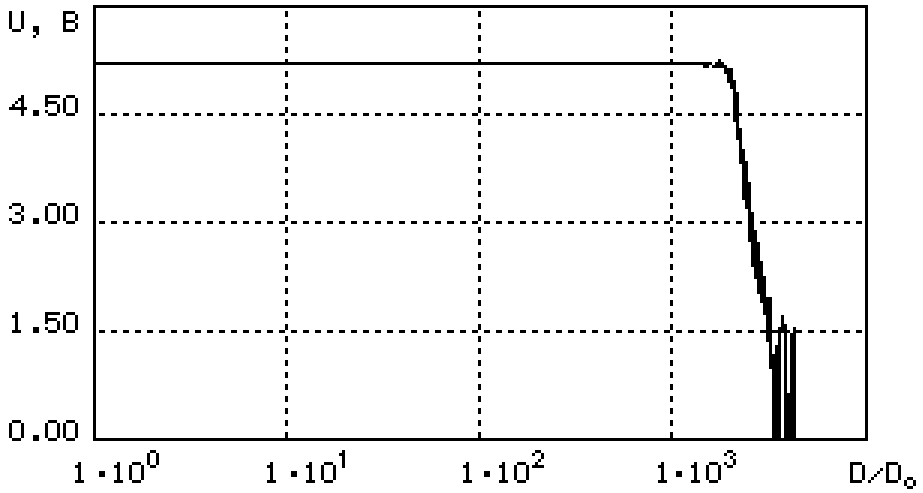


Рисунок 1– Дозовая зависимость выходного напряжения высокого уровня КМОП инвертора 564ЛН2
(Fig. 1– Dose-dependent output voltage high-level CMOS inverter 564ЛН2)

Одновременно производился функциональный контроль ЭСППЗУ, по результатам которого рассчитана функция работоспособности Ψ (отношение числа неисправных ячеек памяти к их общему числу), также изображенная на рисунке 2. Видно, что о работоспособности ЭСППЗУ можно достаточно точно судить по изменению уровня логического "0".

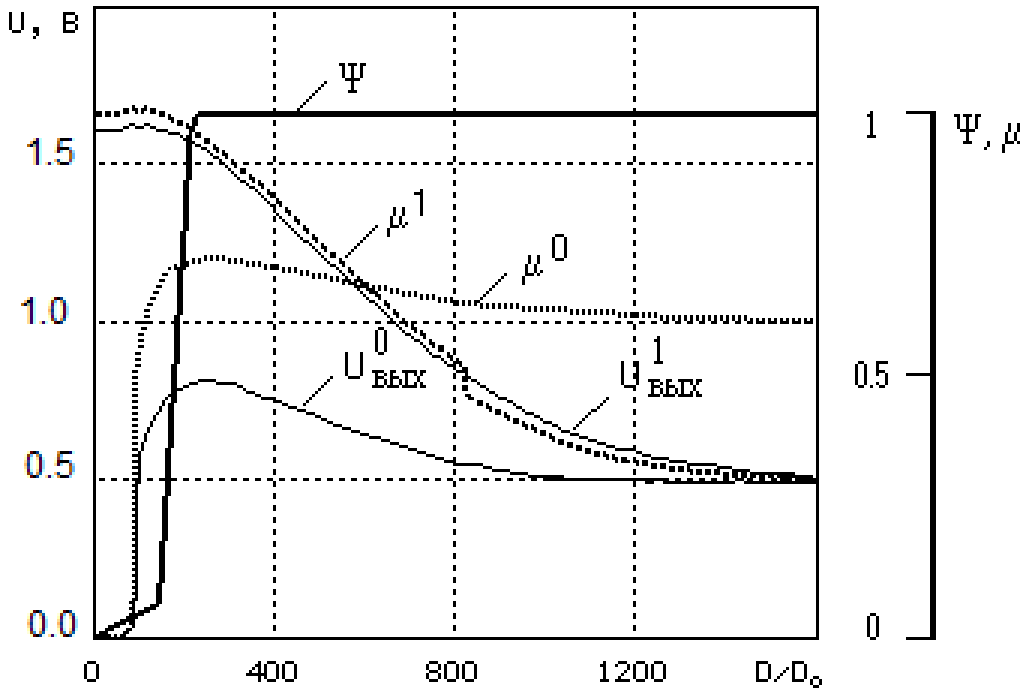


Рисунок 2 – Зависимости напряжений выходных логических уровней "0" и "1" СФ-блока ЭСППЗУ от поглощенной дозы и критериальные функции принадлежности
(Fig. 2 – Dependence of the stress output logical levels "0" and "1" SF-block from the absorbed dose and criteria-based membership function)

В ряде случаев важным критериальным параметром работоспособности может служить ток потребления. В качестве примера на рисунке 3 показана дозовая зависимость тока потребления СФ-блока процессора вместе с моментом наступления функционального

отказа процессора, который, как видно, практически совпадает с моментом резкого возрастания тока[10,11].

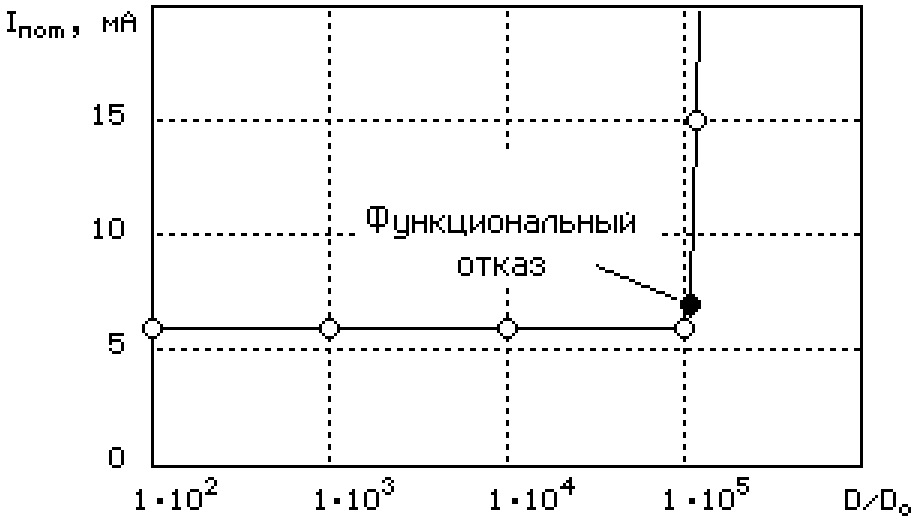


Рисунок 3 – Дозовая зависимость статического тока потребления и момент функционального отказа СФ-блока процессора
(Fig. 3 - Dose dependence of the static current consumption and the time of functional failure of the SF-block of the processor)

Анализ особенностей функциональных дозовых отказов микросхем и СФ-блоков ОЗУ показал, что в ряде случаев они проявляются как "залипание" ячеек памяти в одно из логических состояний, причем разные ячейки отказывают при существенно разных уровнях воздействия [12]. На рисунке 4показана зависимость числа отказавших ячеек от времени воздействия в режиме "хранение 1" (отдельно ложные "0" и "1") СФ-блока оперативного запоминающего устройства (ОЗУ) организацией 4К х 1. Для функционально-логического моделирования таких отказов можно воспользоваться нечеткой логической моделью, показанной на рисунке 5.

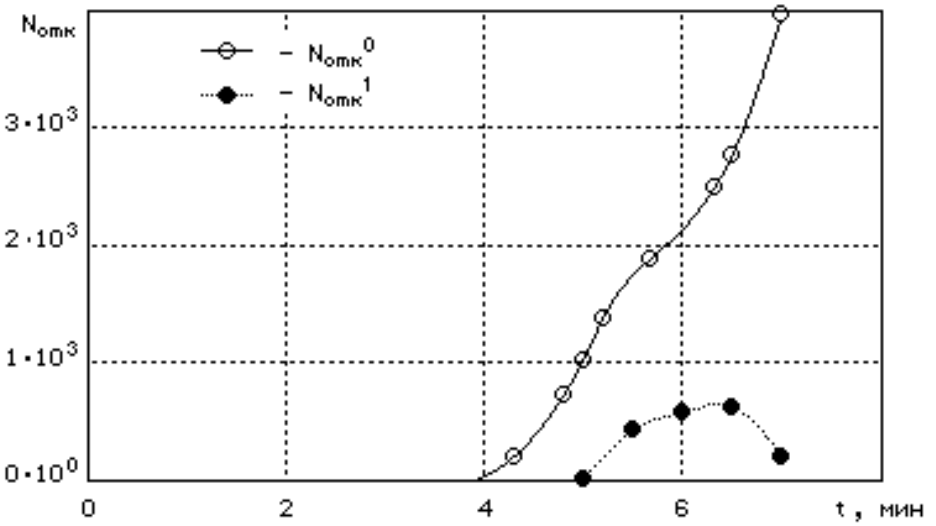


Рисунок 4– Зависимости числа отказавших ячеек памяти СФ-блока ОЗУ от времени облучения
(Fig. 4– Dependence of the number of failed memory cells of SF-block RAM from the time of exposure)

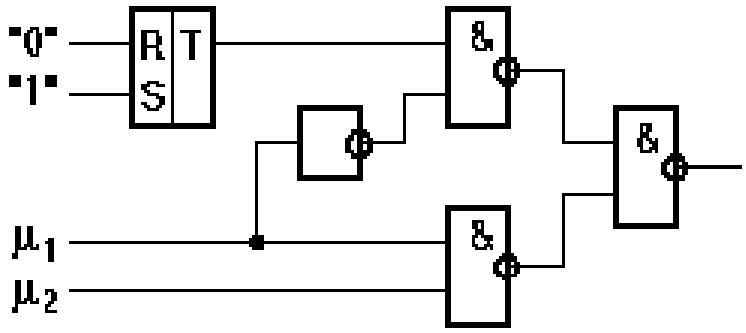


Рисунок 5 – Нечеткая логическая модель отказов ячеек памяти
(Fig. 5 – the Fuzzy logical model of failure memory cells)

Здесь ячейка памяти ОЗУ изображена в виде триггера, а радиационный отказ моделируется введением двух функций принадлежности – μ_1 и μ_2. Функция μ_1 отражает степень выхода ОЗУ из строя и является, по сути, функцией ее работоспособности. Функция μ_2 характеризует тип отказа. Для определения этих функций можно воспользоваться соотношениями:

$$\mu_1(D) = \frac{N^0_{\text{отк}}(D)+N^1_{\text{отк}}(D)}{N} \quad (1),$$

$$\mu_2(D) = \frac{N^1_{\text{отк}}(D)}{N^0_{\text{отк}}(D)+N^1_{\text{отк}}(D)} = \frac{N^1_{\text{отк}}(D)}{\mu_1(D)\cdot N} \quad (2),$$

где $N_{отк}^0(D)$ и $N_{отк}^1(D)$ – зависимость от уровня воздействия числа отказов типа "ложный 0" и "ложная 1" соответственно, N – число ячеек памяти. На рисунке 6 показаны полученные по этим соотношениям для зависимости рисунка 4 функции принадлежности.

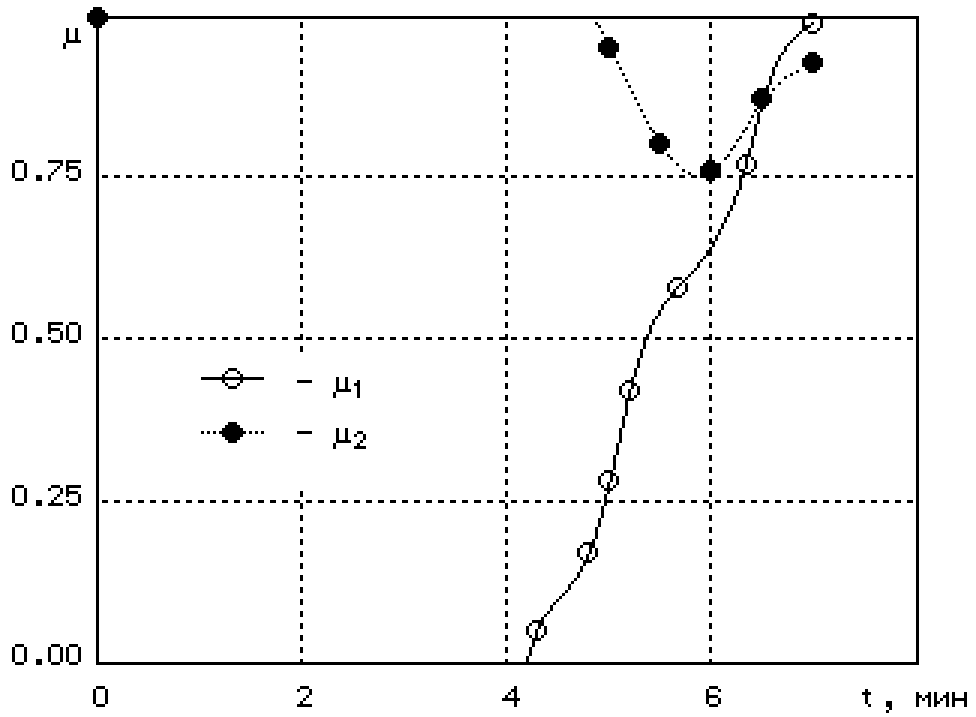


Рисунок 6– Функции принадлежности нечеткой модели отказа ячеек памяти СФ-блока ОЗУ
(Fig. 6– Membership functions of a fuzzy model of failure memory cells SF-block RAM)

Очевидно, что зависимости, подобные изображенным на рисунке 6, но полученные при облучении в режиме "хранение 0", были бы совершенно другими – имело бы место "залипание" ячеек в "0". Это отразилось бы на функции типа отказа μ_2. Таким образом, при моделировании необходимо учитывать влияние режима функционирования в процессе облучения на параметры моделей.

СПИСОК ЛИТЕРАТУРЫ:

1 В.Немудров, Г.Мартин. Системы-на-кристалле. Проектирование и развитие. М.: Техносфера, 2004. – 216 с.
2 А.Ю. Никифоров, В.А. Телец. Радиационная стойкость электронной компонентной базы систем специальной техники и связи. Спецтехника и связь, 2011, № 4-5, с. 2-3.
3 О.А. Калашников, П.В. Некрасов, А.Ю. Никифоров, и др. Системы на кристалле: особенности радиационного поведения и оценка радиационной стойкости. Микроэлектроника, 2016, том 45, №1, С. 36-43.
4 А.Ю. Никифоров, П.К. Скоробогатов, М.Н. Стриханов, В.А. Телец, А.И. Чумаков. Развитие базовой технологии прогнозирования, оценки и контроля радиационной стойкости изделий микроэлектроники. Известия вузов. Электроника, 2012, № 5 (97), с. 18-23.
5 Д.В. Бобровский, Г.Г. Давыдов, А.Г. Петров, и др. Реализация базовых методов радиационных испытаний ЭКБ на основе аппаратно-программного комплекса аппаратуры National Instruments. Известия вузов. Электроника, №5(97), 2012, С. 91-104.
6 О.А. Калашников. Расчетно-экспериментальное моделирование дозовых радиационных функциональных отказов цифровых СБИС. Безопасность информационных технологий, 2016-3, С. 34-39.
7 Е.Р. Аствацатурьян, В.А. Беляев, Н.С. Трушкин. Функционально-логическое моделирование радиационного поведения цифровых устройств. Препринт МИФИ, 016-93, 1993, 28 с.
8 Г.Г. Давыдов, А.В. Согоян, А.Ю. Никифоров, и др. Методика оперативного неразрушающего контроля дозовой стойкости КМОП БИС на КНС структурах. Микроэлектроника, 2008, том 37, № 1, с. 67-77.
9 А.Б. Боруздина, А.В. Уланова, Н.Г. Григорьев, А.Ю. Никифоров. Дозовая деградация динамических параметров микросхем памяти. Микроэлектроника, 2012, т. 41, № 4, с. 284-290.
10 П.В.Некрасов, А.А.Демидов, О.А.Калашников. Функциональный контроль микропроцессоров при проведении радиационных испытаний. Приборы и техника эксперимента, № 2, Март-Апрель 2009, С. 48-52.
11 Д.В.Бобровский, В.С.Волин, П.В.Некрасов, О.А.Калашников, Ю.С.Рябцев. Радиационная стойкость микропроцессоров семейства "МЦСТ-R". Вопросы радиоэлектроники, серия ЭВТ, выпуск 3, 2010 г.
12 В.В. Елесин, Г.Н. Назарова, Г.В. Чуков, Ю.А. Кабальнов, А.А. Титаренко. Исследование возможности разработки радиационно-стойких БИС навигационного назначения по отечественной КМОП КНИ технологии с нормами 0.35 мкм. Микроэлектроника, 2012, т. 41, № 4, с. 291-303.

REFERENCES:

[1] V.Nemudrov, G.Martin. System-on-chip. The design and development.. M.: Tehnosfera, 2004. – 216 p. (In Russian).
[2] A.Yu. Nikiforov, V.A. Telets. Radiation resistance of electronic component base systems special technology and communication. Spetstehnika i svyaz, 2011, N 4-5, p. 2-3. (In Russian).
[3] O.A. Kalashnikov, P.V. Nekrasov, A.Yu. Nikiforov, and other. System on a chip: the features of the radiation behavior of the radiation resistance. Mikroelektronika, 2016, tom 45, N1, P. 36-43. (In Russian).
[4] A.Yu. Nikiforov, P.K. Skorobogatov, M.N. Strihanov, V.A. Telets, A.I. Chumakov. The development of basic technology forecasting, assessment and control of radiation resistance of microelectronic devices. Izvestiya vuzov. Elektronika, 2012, N 5 (97), p. 18-23. (In Russian).
[5] D.V. Bobrovskiy, G.G. Davyidov, A.G. Petrov, and other. Implementation of basic methods of radiation tests of electronic components based on hardware and software equipment National Instruments. Izvestiya vuzov. Elektronika, N 5(97), 2012, P. 91-104. (In Russian).
[6] O.A. Kalashnikov. Experiment-calculated modeling of radiation dose functional failures of digital VLSI. Bezopasnost` Informatsionnykh Tekhnologiy ISSN: 2074-7128 (Print); ISSN: 2074-7136 (On-Line), v.23, N3(2016), P. 34-39. (In Russian).
[7] E.R. Astvatsaturyan, V.A. Belyaev, N.S. Trushkin. Functional logic simulation of radiation behavior of digital devices. Preprint MIFI, 016-93, 1993, 28 p. (In Russian).
[8] G.G. Davyidov, A.V. Sogoyan, A.Yu. Nikiforov, i dr. The technique of rapid non-destructive testing dose resistance of CMOS IC at the SPS structures. Mikroelektronika, 2008, tom 37, N 1, p. 67-77. (In Russian).
[9] A.B. Boruzdina, A.V. Ulanova, N.G. Grigorev, A.Yu. Nikiforov. Dose the degradation of the dynamic parameters of the memory chips. Mikroelektronika, 2012, t. 41, N 4, p. 284-290. (In Russian).
[10] P.V. Nekrasov, A.A. Demidov, O.A. Kalashnikov. Functional control of microprocessors during radiation tests. Pribory i itehnika eksperimenta, N 2, Mart-Aprel 2009, P. 48-52. (In Russian).

[11] D.V. Bobrovskiy, V.S. Volin, P.V. Nekrasov, O.A. Kalashnikov, Yu.S. Ryabtsev. Radiation resistance of the microprocessors of the family "MCST-R". Voprosyi radioelektroniki, seriya EVT, vyipusk 3, 2010 g. (In Russian).
[12] V.V. Elesin, G.N. Nazarova, G.V. Chukov, Yu.A. Kabalnov, A.A. Titarenko. A feasibility study on the development of radiation-resistant BIS of the navigation destination at domestic CMOS SOI technology with the norms of 0.35 μm. Mikroelektronika, 2012, t. 41, N 4, p. 291-303. (In Russian).

Поступила в редакцию - 30 июня 2017 г. Окончательный вариант – 01 ноября 2017 г.
Received – June 30, 2017. The final version – November 01, 2017.

Алексей Е. Сулавко[1], Самал С. Жумажанова[1], Алексей А. Нигрей[2], Лала Н. Закутнева[3]
[1]Омский государственный технический университет,
пр-т Мира, 11, г. Омск, 644050, Россия
e-mail: sulavich@mail.ru, ORCID 0000-0002-9029-8028
e-mail: samal_shumashanova@mail.ru, ORCID 0000-0002-6785-5201
[2]Омский государственный университет путей сообщения,
пр-т Маркса, 35, г. Омск, 644046, Россия
e-mail: nigrey.n@mail.ru, ORCID 0000-0002-8391-5374
[3]Снежинский физико-технический институт - филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»,
Комсомольская, 8, г. Снежинск, 456776, Россия
e-mail: zakytnevaln@yandex.ru, ORCID 0000-0002-0910-3618

ВЛИЯНИЕ ПСИХОФИЗИОЛОГИЧЕСКОГО СОСТОЯНИЯ ПОДПИСАНТА НА РЕЗУЛЬТАТЫ ЕГО ИДЕНТИФИКАЦИИ ПО РУКОПИСНОМУ ОБРАЗУ ЕСТЕСТВЕННЫМ И ИСКУССТВЕННЫМ ИНТЕЛЛЕКТАМИ*

DOI: http://dx.doi.org/10.26583/bit.2017.4.10

Аннотация. В настоящее время активно совершенствуются различные механизмы обеспечения информационной безопасности, и особое внимание уделяется предотвращению несанкционированного доступа к информационным ресурсам. Наиболее слабым звеном остается человеческий фактор и процесс идентификации, а также аутентификации пользователя. Совершенствование технологий защиты информационных ресурсов от внутренних угроз безопасности лежит на пути перехода к биометрическим системам скрытой идентификации пользователей компьютера и их психофизиологического состояния. Изменение психофизиологического состояния отражается на почерке человека. В работе проведена оценка влияния состояния утомления и возбуждения подписантов на результаты их идентификации человеком и методами распознавания образов по воспроизводимым подписям. Осуществлено сравнение возможностей естественного и искусственного интеллекта в равных условиях. При изменении состояния подписанта вероятность ошибок его распознавания искусственным интеллектом возрастает в 3,3-3,7 раз. Человек идентифицирует рукописный образ с меньшим числом ошибок, если подписант возбужден, и с большим числом ошибок, если он утомлен.

Ключевые слова: идентификационные признаки, внешний вид подписи, динамика воспроизведения рукописного пароля, алгоритм распознавания образов человеком и автоматом, формула Байеса.

Для цитирования. **СУЛАВКО, Алексей Е. et al.** ВЛИЯНИЕ ПСИХОФИЗИОЛОГИЧЕСКОГО СОСТОЯНИЯ ПОДПИСАНТА НА РЕЗУЛЬТАТЫ ЕГО ИДЕНТИФИКАЦИИ ПО РУКОПИСНОМУ ОБРАЗУ ЕСТЕСТВЕННЫМ И ИСКУССТВЕННЫМ ИНТЕЛЛЕКТАМИ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 87-97, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/284>. Дата доступа: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.10.

Благодарности. Работа выполнена при финансовой поддержке РФФИ (грант №15-07-09053).

Alexey E. Sulavko[1], Samal S. Shumashanova[1], Alexey A. Nigrey[2], Lala N. Zakutneva[3]
[1]Omsk state technical university, pr. Mira, 11, Omsk, 644050, Russia
e-mail: sulavich@mail.ru, ORCID 0000-0002-9029-8028
e-mail: samal_shumashanova@mail.ru, ORCID 0000-0002-6785-5201
[2]Omsk state transport university, pr. Marksa, 35, Omsk, 644046, Russia
e-mail: nigrey.n@mail.ru, ORCID 0000-0002-8391-5374

Snezhinskiy physical technical Institute-branch of federal state autonomous educational institution of higher professional education national research nuclear university "MIFI", Komsomolskaya, 8, Snezhinsk, 456776, Russia
e-mail: zakytnevaln@yandex.ru, ORCID 0000-0002-0910-3618

Influence of the signer's psychophysiological state on the results of his identification using handwritten pattern by natural and artificial intelligence*

DOI: http://dx.doi.org/10.26583/bit.2017.4.10

Abstract. At present, while various mechanisms to ensure information security are actively being improved, particular attention is paid to prevent unauthorized access to information resources. The human factor and process of identification still remain the most problematic, as well as user authentication. A progress in the technology of information resources protection from internal security threats paves its way towards biometric systems of hidden identification of computer users and their psychophysiological state. A change in psychophysiological state results in the person's handwriting. The influence of the signer's state of fatigue and excitation on the results of its identification both by a person and by pattern recognition methods on reproduced signatures are studied. Capabilities of human and artificial intelligence are compared in equal conditions. When the state of the signer changes, the probability of erroneous recognition by artificial intelligence increases by factor 3.3 to 3.7. A person identifies a handwritten image with fewer errors in case when the signer is agitated, and with higher error rate if the signer is tired.
Keywords: identification features, appearance of the signature, password handwriting dynamics, pattern recognition algorithm by human and machine, Bayes' formula.
For citation. **SULAVKO, Alexey E. et al.** Influence of the signer's psychophysiological state on the results of his identification using handwritten pattern by natural and artificial intelligence. IT Security, [S.l.], v. 24, n. 4, p. 87-97, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/284>. Date accessed: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.10.
***Acknowledgement.** The work is executed at financial support of RFBR (grant No. 15-07-09053)

Введение

Совершенствование технологий защиты ресурсов в распределенных информационно-вычислительных системах от внутренних угроз в 21 веке становится определяющим в проблеме информационной безопасности личности, общества, государства. Очередной технологический скачок в решении этой проблемы лежит на пути перехода к биометрическим системам защиты, реализующим технологии скрытой идентификации пользователей компьютера и их психофизиологического, а также эмоционального состояния [1-5]. Такие системы позволяют определить потенциально опасного субъекта при попытке доступа к информационным ресурсам. Одним из видов динамических биометрических образов, позволяющих не только идентифицировать человека, но и его психофизиологическое состояние (ПФС) является рукописный образ пароля или автографа [1].

Проблема повышения надежности систем биометрической идентификации относится к проблемам искусственного интеллекта, т.к. такие системы строятся на базе методов распознавания образов. Один из интересных вопросов, возникающих на пути решения данной проблемы, связан с выбором биометрических параметров, характеризующих идентифицируемых субъектов (признаков). Этот вопрос можно сформулировать следующим образом. Какие признаки использует человек при идентификации рукописных образов? Речь идет не о специалисте-графологе, который руководствуется разработанными методиками, а о неподготовленном человеке. Естественный интеллект является универсальным решателем плохо формализуемых задач, человек интуитивно подбирает варианты решения, сталкиваясь с новой задачей.

Отсюда возникает еще один вопрос: может ли естественный интеллект соревноваться с искусственным при решении задачи биометрической идентификации? Люди легко узнают друг друга по голосу и лицу, если они знакомы и часто видятся (разговаривают). Однако не каждый может с легкостью идентифицировать человека, если контактировал с ним всего один-два раза. Биометрическая система имеет в распоряжении мало информации об идентифицируемом субъекте и должна обучаться всего на нескольких примерах. В настоящей работе произведена попытка сравнения возможностей естественного и искусственного интеллекта при решении задачи идентификации рукописного образа в равных условиях.

Известно, что изменение ПФС отражается на почерке человека [6]. Это можно определить по ряду признаков. Однако на данный момент нет данных относительно того, влияют ли изменения почерка, вызванные утомлением или возбуждением субъекта на возможность его идентификации методами искусственного интеллекта и естественным интеллектом человека. В данной работе проводится оценка влияния ПФС подписантов на результаты их идентификации по воспроизводимым подписям человеком и методами распознавания образов.

Решаемые в рамках работы задачи играют роль вспомогательных в контексте проблемы повышения надежности биометрической аутентификации по рукописному паролю и подписи. Однако их решение представляет интерес, так как оно позволит сделать первый шаг на пути создания системы идентификации человека с учетом его психофизиологического состояния. Такая система может не только правильно установить личность субъекта, но и распознать в нем потенциального нарушителя.

Формирование выборки рукописных образов подписантов, находящихся в различных ПФС

Для проведения эксперимента по оценке влияния факторов утомления и возбуждения субъектов на результаты их идентификации требуется сформировать выборку образцов контрольного рукописного слова, вводимого испытуемыми, находящимися в этих состояниях. В качестве контрольных слов использовались: «Безопасность», «Авторизация», «Идентификация», «Экранирование». Под психофизиологическим состоянием (ПФС) обычно понимается совокупность свойств человека, отражающих биологические аспекты проявления адаптации к изменяющимся условиям окружающей среды и оцениваемых на основании измерения психофизиологической информации [7]. Под влиянием окружающей среды в данном контексте подразумевается любое воздействие, которое приводит к изменениям в психике или вызывает физиологический отклик организма субъекта.

Сложность научной проработки данного вопроса состоит в том, что в физиологии нет единства взглядов по кардинальным вопросам проблемы утомления: о центрально-нервном или периферическом, локальном характере возникновения мышечного утомления, о биологическом значении утомления. Имеется 4 основных теории появления усталости (утомления): теория истощения (растрата энергетических ресурсов органов человека), засорения (следствие накопления в организме продуктов обмена веществ), отравления (накопление в теле человека кенотоксина, вызывающего функциональные расстройства в организме) и опьянения. Первые 3 относят причину возникновения усталости к мышечному утомлению, которое влияет только на характеристики движений: координацию, точность и темп. Последняя теория объясняет причину утомления изменениями, происходящими в центральной нервной системе, вызвать которые можно употребив алкоголь. В этом случае усталость влияет также на эмоциональную сферу субъекта и также ведет к снижению работоспособности. Наиболее серьезной считается трактовка утомления как физиологического состояния организма, вызванного интенсивной или длительной деятельностью и выражающегося во временном снижении работоспособности.

При формировании базы паролей были привлечены 10 человек, каждый из которых по 50 раз написал каждое из указанных контрольных слов на графическом планшете Wacom в трех ПФС (всего 2000 образцов, по 500 на каждое слово):

1. Спокойное состояние. Испытуемый не подвергался каким-либо воздействиям.
2. Состояние утомления. Эксперимент по сбору данных проводился в отдельный день в конце рабочего дня. Испытуемый подвергался интенсивной физической нагрузке, после чего субъект принимал 25-100 мл водки (в зависимости от массы тела и пола, требовалось обеспечить содержание спирта в крови порядка 0,31-0,89‰, так как данный уровень опьянения приводит к снижению внимания, увеличению времени реакции[8]).
3. Состояние возбуждения. Испытуемый принимал кофе и вдыхал пары нашатырного спирта непосредственно перед написанием контрольных слов.

В процессе ввода рукописных образов за испытуемыми осуществлялся холтер-мониторинг частоты сокращений сердечной мышцы (рис. 1) и регистрировались следующие функции, зависящие от времени:

– функция изменения координаты x при письме, $x(t)$;
– функция изменения координаты y при письме, $y(t)$;
– функция давления кончика пера на поверхность планшета при письме, $p(t)$.

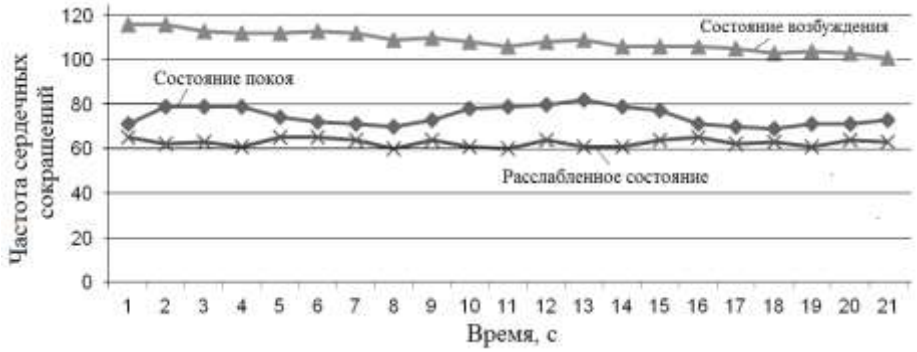


Рисунок 1 - Частота сердечных сокращений одного их испытуемых в различных психофизиологических состояниях
(Fig. 1. - Heart rate is one of the subjects in various physiological States)

Биометрические признаки рукописных образов, используемые при автоматическом распознавании подписантов

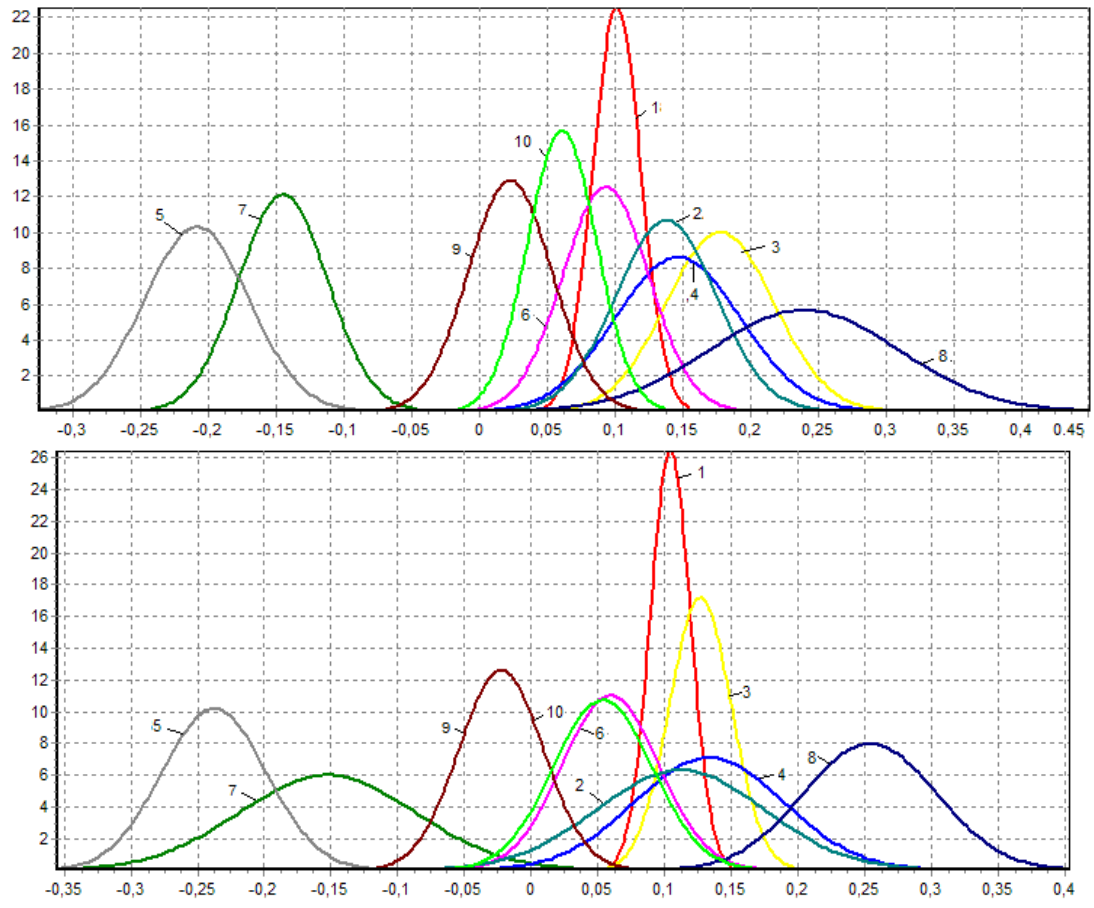
Надежность системы идентификации характеризуется вероятностями ошибок 1-ого (ошибочное признание известного системе субъекта за неизвестного) и 2-ого рода (ошибочное признание неизвестного субъекта за известного) и напрямую зависит от информативности идентификационных признаков. К обоим типам ошибки можно отнести ошибочное признание одного известного субъекта за другого известного системе субъекта. Для поиска и выбора оптимального пространства признаков применяются различные методы и подходы. При анализе графических образов находят применение формальный имитационный метод Блока, Нильсона и Дуды, имитационный метод Ура и Восслера [9]. Для выделения признаков динамики подписи или рукописного пароля успешно применяется спектральный, корреляционный и вейвлет-анализ исходных сигналов рукописного образа (функций координат, давления и наклона пера) [1, 10], при этом учитываются особенности предметной области (возможный диапазон частот колебания руки подписанта, параметры устройства ввода рукописного образа и т.д.). Часто размерность пространства признаков стараются снизить, применяя факторный анализ, в частности, метод главных компонент [11]. Последнее время при выборе биометрических признаков для распознавания субъектов популярной становится противоположная идеология, в соответствии с которой размерность признаков стоит повышать (даже если признаки сильно взаимозависимы) [12]. В настоящем исследовании

использовались признаки, получение которых из рукописного образа подробно описано в работах [11, 13, 14]:

- нормированные по энергии амплитуды 16 самых низкочастотных гармоник функции давления $p(t)$.
- нормированные по энергии амплитуды 16 самых низкочастотных гармоник функции скорости пера $v_{xy}(t)$.
- коэффициенты корреляции между функциями $x(t)$, $y(t)$, $p(t)$ и их производными.
- расстояния между некоторыми точками подписи в трехмерном пространстве (точки выбираются равномерно с некоторым шагом, далее находятся расстояния между всеми парами этих точек, третье измерение — давление пера на планшет).
- характеристики изображения подписи: отношение длины подписи к ее ширине, центр подписи, угол наклона подписи, угол наклона между центрами половин подписи.
- коэффициенты вейвлет-преобразований Добеши по базису D6 функций $v_{xy}(t)$ и $p(t)$.

Большинство указанных признаков имеют распределение, близкое к нормальному, реже к логнормальному или распределению Лапласа (двойному экспоненциальному), что проверялось критерием согласия Хи-квадрат. Поэтому в качестве эталонной информации о признаке целесообразно хранить параметры функции плотности вероятности значений признака.

Анализ введенных образцов показал, что в измененном состоянии среднеквадратичное отклонение значений многих признаков возрастает, т.е. стабильность воспроизведения некоторых особенностей подписи снижается (рис. 2), однако это не является общим правилом для всех признаков. Математическое ожидание низкочастотных амплитуд функций $p(t)$ и $v_{xy}(t)$ в измененном состоянии чаще всего возрастает, т.е. доля низкочастотных колебаний руки при вводе автографа у большинства испытуемых увеличивается.



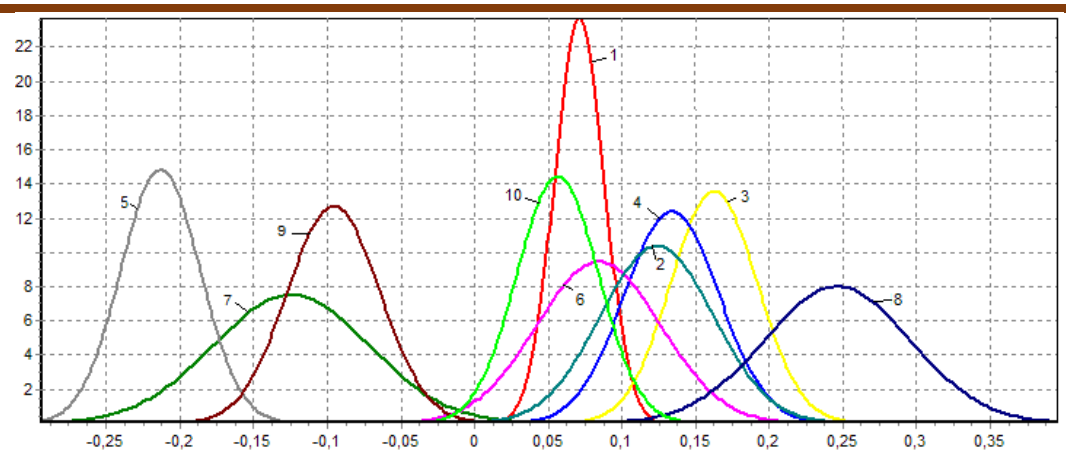


Рисунок 2 - Графики функций плотностей вероятности коэффициентов корреляции функций x(t)и y(t) для 10 испытуемых (цифры на графике от 1 до 10) в различных психофизиологических состояниях: а) – покоя, б) - возбуждения и в) расслабления
(Fig. 2 - Graphs of the probability densities of ratios of correlation functions x(t)and y(t) for 10 subjects (numbers on the chart from 1 to 10) in various physiological States: a) rest, b) excitation and b) relaxing)

Эксперимент по распознаванию образов контрольных рукописных слов методами искусственного интеллекта

В [15] предложено несколько алгоритмов формирования решений в системах идентификации в пространстве малоинформативных признаков. По результатам опытов [15] наилучшим из предложенных оказался метод последовательного применения формулы гипотез Байеса (ППФБ), в [16] данный метод был усовершенствован. Метод ППФБ заключается в вычислении интегральных апостериорных вероятностей гипотез за некоторое число шагов, равное количеству признаков при помощи модифицированной формулы гипотез Байеса (1). Каждая гипотеза подразумевает, что предъявляемые данные о подсознательных движениях принадлежат определенному субъекту, т.е. каждая гипотеза ассоциируется с определенным эталоном испытуемого. На каждом шаге за априорную вероятность принимается апостериорная вероятность, вычисленная на предыдущем шаге. На первом шаге все гипотезы считаются равновероятными, т.е. $P_0(H_i/A) = 1/n$, где n – количество гипотез. Условные вероятности $P(A_j/H_i)$ вычисляются исходя из закона распределения значений признаков, как плотности вероятности значений признаков предъявленных субъектом в процессе идентификации [15, 16]. Решение о принадлежности вектора значений признаков к одному из эталонов принимается на каком-либо шаге, когда апостериорная вероятность одной из гипотез преодолевает пороговое значение (подбираемое заранее по аналогии с работами [2, 5, 16]) в пользу данной гипотезы (ее апостериорная вероятность будет максимальной). Если ни одна из гипотез не преодолела порог, образ считается нераспознанным, т.е. неизвестным.

$$P_j(H_i|A) = P_{j-1}(H_i|A) + \left(\frac{P_{j-1}(H_i|A)P(A_j|H_i)}{\sum_{i=1}^{n} P_{j-1}(H_i|A)P(A_j|H_i)} - P_{j-1}(H_i|A) \right) \times \left(W_j\right) \quad (1),$$

где: W_i вес j-го признака, $P_j\ (H_i/A)$ – апостериорная вероятность i-ой гипотезы, вычисляемая на j-ом шаге при поступлении j-ого признака, $P(A_j/H_i)$ – условная вероятность i-ой гипотезы при поступлении j-ого признака. Вес признака W_i вычисляется по формуле (2) и характеризует его информативность на j-ом шаге алгоритма

последовательного применения формулы Байеса, подробно данный вопрос раскрывается в [16].

$$W_j = 1 - \sum_{i=0}^{n} P_{j-1}(H_i|A) Sum_{ji} \quad (2),$$

где: Sum_{ji} – площадь пересечения функции распределения значений j-ого признака для i-ой гипотезы с функциями распределения значений данного признака для других гипотез. При $W_i = 1$ получим классическую формулу гипотез Байеса.

В процессе эксперимента увеличивалось количество гипотез от 2 до 5. Эксперимент повторялся в 3-х вариантах: сначала для распознавания использовались рукописные образы, полученные в состоянии покоя, потом в состоянии усталости, далее в состоянии возбуждения. При этом во всех случаях для обучения метода ППФБ использовались подписи, полученные в состоянии покоя. Получены следующие результаты:

- в спокойном состоянии сумма вероятностей ошибок идентификации 1-ого и 2-ого рода составила от 0,005 до 0,01 в зависимости от количества образов известных системе;
- при идентификации по подписи в состоянии утомления вероятность ошибочных решений возрастает в среднем в 3,7 раз;
- при идентификации по подписи в состоянии возбуждения вероятность ошибочных решений возрастает в среднем в 3,3 раза.

Вероятность ошибок определялось как отношение их числа к общему количеству опытов.

Эксперимент по распознаванию образов контрольных рукописных слов людьми

В качестве испытуемых, распознающих образы рукописных слов, были привлечены молодые люди (студенты, не принимавшие участия в написании рукописных паролей) в возрасте от 18 до 25 лет, мужчины и женщины в равном соотношении, число которых составляло 50 человек. Испытуемые были мотивированы на добросовестное выполнение задания, данного им в рамках эксперимента. При сравнении способностей естественного интеллекта с искусственным необходимо воссоздать максимально равные условия: равный объем обучающей выборки и сравнимое количество информации, содержащейся в обучающих и тестовых примерах.

На этапе обучения испытуемых на экране монитора одна за другой формировались 20 случайных реализаций рукописного слова определенного человека в темпе их получения на графическом планшете. При этом сила нажатия пера на планшет обозначалась через яркость соответствующих фрагментов рукописного образа: чем сильнее нажатие, тем темней линии. Испытуемые запоминают особенности предъявляемого образа, чтобы в будущем отличить данный образ от образов рукописных слов других людей.

На этапе идентификации рукописных образов на экране в случайном порядке в различном темпе (быстрей, медленней, в темпе написания субъектом) формировались рукописные образы, не использованные при обучении. Испытуемые, наблюдая за их воспроизведением, принимали решение, кому принадлежит представленное слово. Для фиксирования решений каждому испытуемому был дан специальный бланк. По окончанию эксперимента подсчитывалось число ошибок, и определялась их вероятность как отношения числа ошибок соответствующего рода к общему количеству опытов.

Эксперимент повторялся несколько раз, при этом каждый раз увеличивалось количество распознаваемых образов (от одного до пяти), т.е. сначала испытуемые запоминали особенности воспроизведения слова одним определенным субъектом, потом особенности воспроизведения этого же слова двумя субъектами и т.д. Таким образом, имитировалось повышение количества формируемых эталонов. Распознаваемые образы также менялись. Результаты эксперимента можно видеть на рис. 3-6 (первый столбик –

усталое состояние (алкогольное опьянение), второй – возбужденное состояние (воздействие нашатырным спиртом), нормальное состояние (без воздействий)).

Рисунок 3 - Изменение вероятности ошибочного не опознавания известного субъекта при увеличении количества субъектов во время обучения
(Fig. 3 - The Change in the probability of incorrect identification not known subject with increasing number of subjects while learning)

Рисунок 4 - Изменение вероятности ошибочного опознавания неизвестного субъекта при увеличении количества субъектов во время обучения
(Fig. 4 - The Change in the probability of incorrect identification of the unknown entity when the number of subjects during training)

Рисунок 5 - Изменение вероятности ошибочного отнесения одного известного субъекта к другому известному субъекту количества субъектов во время обучения
(Fig. 5 - The Change in the probability of incorrect classification as a well-known subject to the other famous subject of a number of subjects during training)

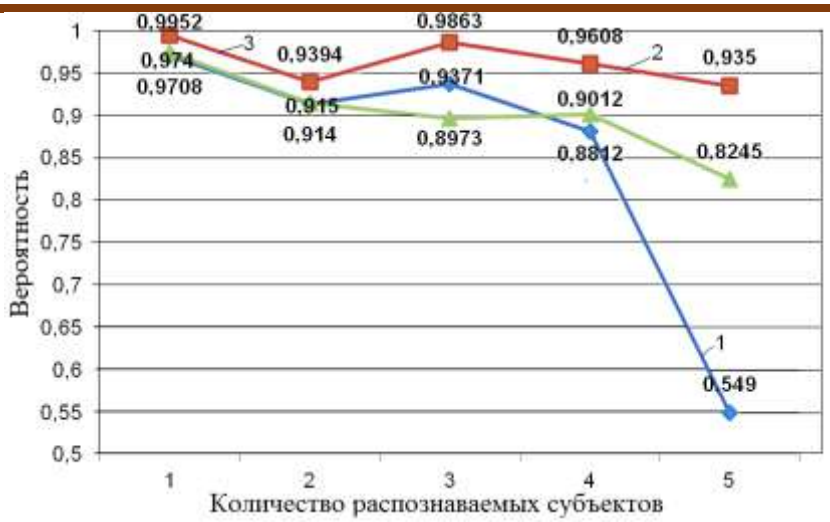


Рисунок 6 - Изменение вероятности верного распознавания субъекта при увеличении количества субъектов во время обучения
(Fig. 6 - The Change in the probability of correct recognition of the subject with increasing number of subjects while learning)

По приведенным рисункам видно, что для состояния возбуждения вероятности ошибок идентификации ниже, чем в спокойном состоянии. Наоборот, в состоянии усталости, вероятность ошибочных решений выше. Это означает, что информативность признаков, которые использует естественный интеллект, повышается, когда состояния испытуемого (распознаваемого субъекта) меняется на возбужденное. В состоянии возбуждения он становится более собранным и внимательным, а его движения становятся более точными. Состояние усталости оказывает на подсознательную сферу испытуемого субъекта обратное воздействие, при этом информативность признаков воспроизводимых паролей снижается.

Анализ результатов

Признаки, которые были использованы для идентификации субъектов автоматом, содержат информацию, как о самом субъекте, так и о его психоэмоциональном состоянии (как состоянии усталости, так и возбужденности и т.д.). Естественный интеллект использует иные признаки. Они содержат информацию о самом субъекте, при этом количество и качество данной информации зависит от психофизиологического состояния субъекта в момент написания рукописного слова (пароля, подписи) – чем субъект сосредоточеннее, более возбужден и сконцентрирован, тем больше информации, которую может воспринять естественный интеллект, содержит о нем его почерк.

Также можно видеть, что искусственный интеллект существенно превосходит естественный при распознавании в режиме идентификации. Вычислительный эксперимент показал, что с увеличением количества идентифицируемых образов разница в количестве ошибочных решений при изменении психофизиологического состояния становится менее ощутимой.

Заключение

Была выдвинута гипотеза: изменения в психофизиологическом состоянии субъекта отражаются на его почерке, что влияет на результаты его идентификации искусственным и естественным интеллектом. Для проверки данной гипотезы был проведен эксперимент по распознаванию субъектов по фрагментам воспроизводимых на экране паролей людьми, а также вычислительный эксперимент по распознаванию субъектов методом последовательного применения модифицированной формулы гипотез Байеса.

Результаты экспериментов говорят о том, что психофизиологическое состояние субъекта влияет на результаты идентификации рукописных образов как искусственным,

так и естественным интеллектами, но по-разному. Естественный интеллект использует признаки, опирающиеся на индивидуальность темпа ввода подписей субъектами. Данные признаки тем стабильнее в почерке, чем более возбужден субъект.

На идентификационные решения, сделанные искусственным интеллектом, любые изменения в психоэмоциональном состоянии субъекта влияют отрицательно (вероятность ошибок возрастает в 3,3-3,7 раз).

Существует точка зрения, что при поиске решений задач из области искусственного интеллекта, стоит ориентироваться на естественный аналог в живой природе. Однако по результатам эксперимента естественный интеллект существенно уступает искусственному по надежности распознавания рукописных паролей. Таким образом, биометрические системы аутентификации (идентификации) субъектов по рукописным паролям превзошли аналог из живой природы. Для дальнейшего повышения надежности требуется идти по пути увеличения вычислительных мощностей (повышения количества признаков, количества и сложности вычислительных узлов алгоритма принятия решений).

СПИСОК ЛИТЕРАТУРЫ:

1 Сулавко А.Е., Еременко А.В., Левитская Е.А., Самотуга А.Е. Идентификация психофизиологических состояний подписантов по особенностям воспроизведения автографа // Информационно-измерительные и управляющие системы. 2017. №1. С. 40–48.

2 Vasilyev V.I., Sulavko A.E., Eremenko A.V., Zhumazhanova S.S. Identification potential capacity of typical hardware for the purpose of hidden recognition of computer network users // X International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics), Omsk, 15-17 november 2016, pp. 1-5. DOI: 10.1109/Dynamics.2016.7819106.

3 Ложников П.С., Сулавко А.Е., Толкачева Е.В., Жумажанова С.С. Распознавание водителей и их функциональных состояний по обычному и тепловому изображениям лица // Труды научно-технической конференции кластера пензенских предприятий, обеспечивающих безопасность информационных технологий. Том 10, Пенза, 2016. С. 63–65, (http://ПНИЭИ.РФ/activity/science/BIT/T10-p63.pdf).

4 Васильев В.И., Ложников П.С., Сулавко А.Е., Еременко А.В. Технологии скрытой биометрической идентификации пользователей компьютерных систем // Вопросы защиты информации. 2015. № 3 (110). С. 37–47.

5 Сулавко А.Е., Еременко А.В., Левитская Е.А. Разграничение доступа к информации на основе скрытого мониторинга действий пользователей в информационных системах: портрет нелояльного сотрудника // Известия Транссиба. 2015. № 1(21). С. 80–89.

6 Нигрей А.А. Исследование изменения динамики подписи подписанта на графическом планшете при изменении его психофизиологического состояния // Безопасность городской среды: Материалы IV Международной научно-практической конференции (Россия, Омск, 16-18 нояб. 2016 г.). Омск: ОмГТУ, 2017. С. 383–385.

7 Богомолов А.В., Гридин Л.А., Кукушкин Ю.А., Ушаков И.Б. Диагностика состояния человека: математические подходы. М.: Медицина, 2003. 464 с.

8 Федеральные правила полетов (США) 91.17: Алкоголь и пилотирование (Режим доступа: http://flightphysical.com/pilot/alcohol.htm, дата обращения: 16.05.2017).

9 Uhr L., Vossler C. A pattern recognition program that generates, evaluates and adjusts its own operators, в сб. «Computers and thought» под ред. Feigenbaum E., Feldman J., New Yo r k. (Русский перевод в сб. «Вычислительные машины и мышление» под ред. Фейгенбаума Э. И. Фельдмана Дж. М.: Мир, 1967).

10 Иванов А.И. Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции. Пенза: Изд-во ПНИЭИ, 2016. 133 с.
URL: http://пниэи.рф/activity/science/ BOOK16.pdf.

11 Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Volkov D.A. Methods of Generating Key Sequences based on Parameters of Handwritten Passwords and Signatures // Information. 2016. №7. P. 59. DOI: 10.3390/info7040059.

12 Харман Г. Современный факторный анализ. М.: Статистика, 1972. 489 с.

13 Ложников П.С., Сулавко А.Е., Еременко А.В., Волков Д.А. Экспериментальная оценка надежности верификации подписи сетями квадратичных форм, нечеткими экстракторами и персептронами // Информационно-управляющие системы. 2016. №5. С. 73–85.

14 Сулавко А.Е., Еременко А.В., Толкачева Е.В., Борисов Р.В. Комплексирование независимых биометрических признаков при распознавании субъектов на основе сетей квадратичных форм, персептронов

и меры ХИ-модуль // Информационно-управляющие системы. 2017. № 1. С. 50–62. DOI: 10.15217/issn1684-8853.2017.1.50.
15 Епифанцев Б.Н., Ложников П.С., Сулавко А.Е. Сравнение алгоритмов комплексирования признаков в задачах распознавания образов // Вопросы защиты информации. 2012. № 1. С. 60–66.
16 Епифанцев Б.Н., Ложников П.С., Сулавко А.Е. Алгоритм идентификации гипотез в пространстве малоинформативных признаков на основе последовательного применения формулы Байеса // Межотраслевая информационная служба. 2013. № 2. С. 57–62.

REFERENCES:

[1] Sulavko A.E., Eremenko A.V., Levitskaja E.A., Samotuga A.E. Identifying psychophysiological States of the signatories on the specifics of reproduction autograph. Informacionno-izmeritel'nye i upravljajushhie sistemy. 2017. N1. P. 40–48. (In Russian).
[2] Vasilyev V.I., Sulavko A.E., Eremenko A.V., Zhumazhanova S.S. Identification potential capacity of typical hardware for the purpose of hidden recognition of computer network users. X International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics), Omsk, 15–17 november 2016, pp. 1–5. DOI: 10.1109/Dynamics.2016.7819106.
[3] Lozhnikov P.S., Sulavko A.E., Tolkacheva E.V., Zhumazhanova S.S. Recognition of drivers and their functional States in normal and thermal images of the face. Trudy nauchno-tehnicheskoj konferencii klastera penzenskih predprijatij, obespechivajushhih bezopasnost" informacionnyh tehnologij. Tom 10, Penza, 2016. P. 63–65, (http://pnijei.rf/activity/science/BIT/T10-p63.pdf). (In Russian).
[4] Vasil'ev V.I., Lozhnikov P.S., Sulavko A.E., Eremenko A.V. Tehnologii skrytoj biometricheskoj identifikacii pol'zovatelej komp'juternyh sistem. Voprosy zashhity informacii. 2015. N 3(110). P. 37-47. (In Russian).
[5] Sulavko A.E., Eremenko A.V., Levitskaja E.A. Razgranichenie dostupa k informacii na osnove skrytogo monitoringa dejstvij pol'zovatelej v informacionnyh sistemah: portret nelojal'nogo sotrudnika. Izvestija Transsiba. 2015. N 1(21). P. 80–89. (In Russian).
[6] Nigrej A.A. Study of changes dynamics of the signer's signature on the tablet to change its physiological state. Sbornik materialov II Mezhdunarodnoj nauchno-prakticheskoj konferencii «Rol' tehnicheskih nauk v razvitii obshhestva», 6 March 2017, Kemerovo, 2017. P. 236-239. (In Russian).
[7] Bogomolov A.V., Gridin L.A., Kukushkin Ju.A., Ushakov I.B. Diagnosis of the human condition: mathematical approaches. M.: Medicina, 2003. 464 p. (In Russian).
[8] Federal'nye pravila poletov (SShA) 91.17: Alkogol' i pilotirovanie (Rezhim dostupa: http://flightphysical.com/pilot/alcohol.htm, data obrashhenija: 16.05.2017). (In Russian).
[9] Uhr L., Vossler, C. A pattern recognition program that generates, evaluates and adjusts its own operators. "Computers and thought" ed. by E. Feigenbaum, J. Feldman, New Yo r k. (Russian translation in the collection "computers and thinking" ed. by E. Feigenbaum and I. Feldman George. M.: Mir, 1967).
[10] Ivanov A.I. Multidimensional neural network processing of biometric data with the software reproduction of the effects of quantum superposition. Penza: Izd-vo PNIJeI, 2016. 133 p.
URL: http://pnijei.pf/activity/science/ BOOK16.pdf. (In Russian).
[11] Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Volkov D.A. Methods of Generating Key Sequences based on Parameters of Handwritten Passwords and Signatures. Information. 2016. N 7. P. 59. DOI: 10.3390/info7040059.
[12] Harman G. Modern factor analysis. M.: Statistika, 1972. 489 p. (In Russian).
[13] Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Volkov D.A. Experimental evaluation of the reliability of the verification of the signature networks quadratic forms, fuzzy extractors and perceptrons. Informacionno-upravljajushhie sistemy. 2016. N 5. P. 73–85. (In Russian).
[14] Sulavko A.E., Eremenko A.V., Tolkacheva E.V., Borisov R.V. Aggregation independent of biometric characteristics for recognition of subjects based on networks of quadratic forms, perceptrons and measures CHI-module. Informacionno-upravljajushhie sistemy. 2017. N 1. P. 50–62. DOI: 10.15217.ISSN 1684-8853.2017.1.50. (In Russian).
[15] Epifancev B.N., Lozhnikov P.S., Sulavko A.E. Sravnenie algoritmov kompleksirovanija priznakov v zadachah raspoznavanija obrazov. Voprosy zashhity informacii. 2012. N 1. P. 60–66. (In Russian).
[16] Epifancev B.N., Lozhnikov P.S., Sulavko A.E. Algoritm identifikacii gipotez v prostranstve maloinformativnyh priznakov na osnove posledovatel'nogo primenenija formuly Bajesa. Mezhotraslevaja informacionnaja sluzhba. 2013. N 2. P. 57–62. (In Russian).

Поступила в редакцию - 26 мая 2017 г. Окончательный вариант – 01 ноября 2017 г.
Received – May 26, 2017. The final version – November 01, 2017.

Наталья Г. Милославская, Александр И. Толстой
Национальный исследовательский ядерный университет «МИФИ»
115409, Москва, Каширское шоссе, 31, Россия
e-mail: NGMiloslavskaya@mephi.ru, ORCID 0000-0002-1231-1805
e-mail: AITolstoj@mephi.ru, ORCID 0000-0001-9265-1510

КОМПЕТЕНТНОСТНЫЕ ТРЕБОВАНИЯ СТАНДАРТОВ ISO/IEC К ПРОФЕССИОНАЛАМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Наша динамичная жизнь поставила нас перед необходимостью периодической коррекции разработанных в настоящее время профессиональных компетенций (сформулированы в федеральных государственных образовательных стандартах) и трудовых функций (сформулированы в профессиональных стандартах) для очень популярной области информационной безопасности (ИБ). В таких условиях чрезвычайно важным является своевременная реакция на все новое, которое появляется или будет появляться в современных нормативных документах (прежде всего в стандартах). В данной работе сделан прогноз содержания разрабатываемой международной организацией стандартизации (ISO) проектов стандартов ISO/IEC 27021 и ISO/IEC 19896, которые должны содержать требования к компетентности профессионалов в области систем менеджмента ИБ и к компетентности тестировщиков и оценщиков ИБ. Прогноз сделан с учетом требований, содержащихся в группе стандартов ISO/IEC 27000 и рекомендаций документа «Европейская модель электронной компетентности e-CF 3.0».
Ключевые слова: информационная безопасность, компетентность, профессионал в области информационной безопасности, стандарт ISO/IEC.

Николай С. Егошин, Антон А. Конев, Александр А. Шелупанов
Томский государственный университет систем управления и радиоэлектроники,
пр-т. Ленина, д. 40, г. Томск, 634050, Россия,
e-mail: ens@csp.tusur.ru, ORCID 0000-0003-4770-0701,
e-mail: kaa@keva.tusur.ru, ORCID 0000-0002-3222-9956,
e-mail: saa@keva.tusur.ru, ORCID 0000-0003-2393-6701

ФОРМИРОВАНИЕ МОДЕЛИ НАРУШИТЕЛЯ

Аннотация. Под моделью нарушителя понимаются предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности. Модель нарушителя является важной частью информационной безопасности организации. Важно понимать, что игнорирование или недобросовестное построение модели «для галочки» может серьезно отразиться на сохранности конфиденциальной информации и привести к ее потере. Модель нарушителя носит неформальный характер, и, как следствие, не существует строго однозначной методики по составлению таковой. Множество авторов в научно-технической литературе описывает различные методы классификации нарушителей, меж тем многие специалисты по информационной безопасности, работающие на предприятиях, вынуждены составлять свои нормативно-методические документы, так как существующие модели далеко не всегда удовлетворяют всем особенностям работы организации. Несмотря на то, что многие модели имеют высокий уровень корреляции между классификационными признаками, выработать единую модель до сих пор не удалось. В данной работе предпринимается попытка разработки своей собственной методики формирования модели нарушителя. Перед началом работы были сформированы следующие задачи научно-исследовательской работы: 1) изучить существующие методики построения модели

нарушителя; 2) выявить недостатки существующих методик; 3) разработать модель нарушителя и методику составления перечня наиболее вероятных нарушителей, учитывающую выявленные недостатки. В ходе работы были проанализированы несколько существующих моделей нарушителя, в результате этого были выявлены их недостатки и определены сложности, на которые было обращено внимание при разработке собственной модели нарушителя. В разработанной модели были построены причинно-следственные связи между элементами модели и цепочками предполагаемых последствий, описаны и ранжированы возможные виды предполагаемых нарушителей. Модель позволяет строить более полное описание нарушителя информационной безопасности.
Ключевые слова: модель нарушителя, модель угрозы, информационная безопасность, конфиденциальная информация.

Виктор С. Горбатов[1], Игорь Ю. Жуков[2], Олег Н. Мурашов[2]
[1]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: VSGorbatov@mephi.ru, ORCID 0000-0001-9998-9733
[2]ООО «Национальный мобильный портал»,
Волгоградский пр., 2, офис 36, Москва, 109316, Россия
e-mail: i.zhukov@inbox.ru, ORCID 0000-0002-4429-8799
e-mail: olegxozbox@yandex.ru, ORCID 0000-0002-4467-2170

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ АУТЕНТИФИКАЦИИ И ВЫРАБОТКИ ОБЩЕГО КЛЮЧА КОНТРОЛЬНЫХ УСТРОЙСТВ АВТОТРАНСПОРТА

Аннотация. В работе описывается протокол выработки общего ключа с аутентификацией абонентов, предназначенного для использования в бортовых устройствах (тахографах), которые устанавливаются на транспортные средства с целью обеспечения транспортной безопасности дорожного движения. Данный протокол основан на применении известных отечественных криптографических преобразований и направлен на обеспечение целостности и аутентичности данных, передаваемых по каналу связи между бортовым устройством и картами тахографа, входящими в состав контрольных устройств автотранспортных средств. Протокол разработан в соответствии с рекомендациями Росстандарта по принципам разработки и модернизации шифровальных (криптографических) средств защиты информации, оформлен в виде проекта национального стандарта, предлагаемого для общественного обсуждения и утверждения в установленном порядке. Основным результатом данного исследования является формулирование определенных свойств безопасности, идентичных тем задачам, которые ставит перед собой нарушитель с целью его компрометации. Учет методов компрометации позволяет уже на этапе создания протокола заложить в него структурные особенности, обеспечивающие выполнение заданных свойств безопасности и последующее обоснование их достаточности.
Ключевые слова: безопасность транспорта, бортовое устройство, криптографический протокол, механизмы аутентификации, свойства безопасности

Сергей В. Запечников, Полина О. Кожухова
Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31,г. Москва, 115409, Россия
e-mail: SVZapechnikov@mephi.ru, ORCID 0000-0002-7975-6040
e-mail: PKozhukhova@yandex.ru, ORCID 0000-0002-4004-5209

О КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ СКВОЗНЫХ ЗАЩИЩЕННЫХ СОЕДИНЕНИЙ В МЕССЕНДЖЕРАХ WHATSAPP И TELEGRAM

Аннотация. В статье анализируются возможности повышения стойкости защищенных соединений между пользователями мессенджеров в условиях воздействия внешнего нарушителя и недоверия к провайдеру сервиса. В работе проведено сравнение методов и механизмов криптографической защиты информации, заложенных в основу двух широко распространенных мессенджеров: Telegram и WhatsApp. При этом установлено, что для защиты сквозных соединений в мессенджере Telegram используется протокол MTProto, а в мессенджере WhatsApp — протокол Signal.Изучены особенности реализации мессенджеров на наиболее распространенной мобильной платформе Android, связанные с генерацией случайных чисел. В результате детального анализа каждого из них было выявлено, что лучшим по совокупности свойств безопасности является Signal. Помимо WhatsApp, он используется в ряде других популярных мессенджерах, таких как TextSecure, RedPhone, GoogleAllo, FacebookMessenger, Signal. Выявлены и проанализированы возможные атаки на оба мессенджера. В частности, установлено, что в обоих мессенджерах не защищаются метаданные. Обеспечение безопасности метаданных может стать одной из целей дальнейших исследований.
Ключевые слова: криптография, сквозное соединение, шифрование, WhatsApp, Telegram

Юрий Е. Козлов, Владимир Л. Евсеев
Финансовый университет при Правительстве Российской Федерации
(Финансовый университет),
Ленинградский проспект, 49, Москва, 125993, Россия
e-mail: kozlovye@yandex.ru, ORCID 0000-0002-4448-0232
e-mail: VLevseev@fa.ru, ORCID 0000-0003-3283-3106

МУЛЬТИМОДАЛЬНАЯ ТРЕХМЕРНАЯ ДИНАМИЧЕСКАЯ ПОДПИСЬ

Аннотация. Надежная аутентификация в мобильных приложениях является актуальнейшей задачей информационной безопасности современного общества. В настоящее время человека сложно представить без мобильного устройства, подключенного к сети internet. Кроме того, мобильное устройство может хранить большой объем конфиденциальной информации, начиная от личных фотографий, заканчивая инструментами для банковских операций. Использование жеста в воздухе в качестве методики аутентификации впервые было предложено сотрудниками Университета Райса (США) совместно с компанией Моторола в 2009 году. Эта и остальные работы по созданию и усовершенствованию данной методики указаны во введении к статье. К моменту написания статьи, программа, реализующая один из вариантов методики аутентификации при помощи жеста мобильным устройством, доступна к установке для ОС Android. Однако данная программа не получила большого распространения. Возможно, одна из причин этого - недостаточная надежность методики, которая предполагает, как и ее предыдущие аналоги, использование только одного устройства. В данной статье рассмотрена аутентификация с использованием мультимодальной трехмерной динамической подписи (МТДП), выполняемой двумя независимыми мобильными устройствами. Методика аутентификации с помощью МТДП является

улучшенным вариантом аутентификации при помощи жеста в воздухе. В основной части статьи рассмотрена работа прототипа системы аутентификации на основе МТДП. Описаны основные алгоритмы, реализованные в прототипе, а так же предварительные результаты, полученные при его использовании. Авторы предполагают использование данной методики в любых мобильных приложениях после введения ряда дополнительных усовершенствований, о которых рассказано в заключении.
Ключевые слова: аутентификация, мобильное устройство, акселерометр, персонализированный жест, подпись

Александр В. Кузнецов
Финансовый университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский проспект, 49, Москва, 125993, Россия
e-mail: a.kuznetsov@ntc-vulkan.ru, ORCID0000-0002-7160-1845

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМИЧЕСКОГО АППАРАТА УПРАВЛЕНИЯ СОБЫТИЯМИ БЕЗОПАСНОСТИ И РЕЗУЛЬТАТЫ ЕЕ ПРИМЕНЕНИЯ

Аннотация. В настоящей статье рассматривается актуальная задача в области защиты информации, обусловленная отсутствием алгоритмического аппарата управления событиями безопасности и автоматизации процедур определения набора регистрируемых событий безопасности. В первой части статьи сформулирована постановка математической задачи, подлежащей автоматизации с использованием табличного процессора, в том числе определена целевая функция и её переменные, а также приведены ссылки на источники, содержащие сведения о самом алгоритме решения. Представлено писание предложенного автором программного модуля, реализующего алгоритм определения набора регистрируемых событий безопасности, разработанного на базе табличного процессора, сертифицированного по требованиям безопасности информации Федеральной службой по техническому и экспортному контролю. Представлено описание контрольного примера, подготовленного для тестирования разработанного программного модуля, размерностью 30x20, содержащего 14 вариантов пороговых значений количества зарегистрированных событий безопасности варьировалось. Результаты применения программного модуля подтвердили соблюдение заданных граничных условий задачи, выявили нелинейную зависимость целевой функции от увеличения количества регистрируемых событий безопасности, а также нелинейную зависимость процента регистрируемых событий безопасности от общего исходного количества событий безопасности, подлежащих регистрации на источнике событий. Оценка производительности применения предложенного программного модуля, а именно загрузки центрального процессора, являлась приемлемой (не превысила 33%), что позволяет применять данную программную реализацию для типовых автоматизированный рабочих местах специалистов по защите информации, оснащенных соответствующими табличными процессорами. Предложенный в статье подход к программной реализации различных алгоритмов может быть инвариантен к области применения.
Ключевые слова: событие безопасности, управление событиями безопасности, SIEM, источник событий, табличный процессор

Сергей Б. Козлачков[1], Андрей М. Бонч-Бруевич[1], Сергей В. Дворянкин[2],
Надежда В. Васильевская[3], Александра Л. Селенина[1]
[1]Московский Государственный Технический Университет им. Баумана,
2-я Бауманская, 5, Москва, 105005, Россия
e-mail: ksb.perovo@mail.ru, ORCID 0000-0002-7096-6711
e-mail: 123andryb@mail.ru, ORCID 0000-0002-4453-2979
e-mail: so.zz.va@yandex.ru,ORCID 0000-0002-4280-8214
[2]Финансовый Университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский проспект, 49, Москва, 125993, Россия
e-mail: SVDvoryankin@fa.ru, ORCID 0000-0001-6908-0676
[3]ФСТЭК России, Старая Басманная ул., 17, Москва, 105066, Россия
e-mail: infuzoriavalenoc@yandex.ru, ORCID 0000-0002-0078-8665

НЕКОТОРЫЕ ОСОБЕННОСТИ ФОРМИРОВАНИЯ АКУСТОЭЛЕКТРИЧЕСКОГО КАНАЛА УТЕЧКИ РЕЧЕВОЙ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ

Аннотация. В статье рассмотрены актуальные вопросы оценки защищенности акустоэлектрического канала утечки речевой акустической информации, обусловленные различными физическими принципами функционирования разных типов электромеханических преобразователей.

Проведен анализ возможностей технических средств и методов, используемых при ведении акустической речевой разведки (АР-Р) по соответствующему техническому каналу утечки акустической речевой информации (ТКУРИ).

Особое внимание уделено использованию режима отложенного анализа речевых сообщений (искаженных шумами и помехами), позволяющий значительно повысить качество исходных аудиосигналов. Приведен краткий перечень основных методов шумопонижения, которые могут быть использованы при обработке вторичных сигналов акустоэлектрического канала утечки речевой информации.

Описаны типовые искажения, возникающие в процессе формирования акустоэлектрического канала утечки речевой информации. Рассмотрены характер и степень влияния различных видов искажений на показатели оценки защищенности речевой информации (ЗРИ). Показано, что нелинейные искажения вида «ограничение сверху», наиболее характерные для акустоэлектрического канала утечки, в малой степени снижают разборчивость речи. Наряду со статической моделью речевых сигналов Покровского А.Н., рассмотрена динамическая модель, описываемая фонетической функцией Пирогова А.А. Указаны ограничения статической модели и показан характер влияния динамических признаков на разборчивость речи. Дано объяснение эффектам инвариантности разборчивости речи относительно линейных искажений в канале утечки.

Приведены результаты экспериментальных исследований, в определенной степени, противоречащие некоторым положениям формантной теории разборчивости речи, применяемых для оценки ЗРИ. Определен ряд механизмов повышения помехоустойчивости речевых сообщений, позволяющих выполнять реконструкцию речевых сигналов (РС), искаженных шумами и помехами.

В заключении перечислены предложения по перспективным направлениям совершенствования методов оценки ЗРИ в ТКУРИ.

Ключевые слова: акустическая речевая разведка, акустоэлектрические преобразователи, форманты, фонемы, защита информации, разборчивость речи, речевой сигнал.

Роман А. Устинов
Финансовый университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский пр-т, 49, г. Москва, 125993, Россия
e-mail: public-ura@yandex.ru, ORCID 0000-0002-8454-9951

ОСОБЕННОСТИ СОВРЕМЕННЫХ СИСТЕМ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2017.4.08

Аннотация. На сегодняшний день речевые технологии являются одним из самых активно развивающихся секторов в мировой экономике. В связи с чем, вопросы обеспечения безопасности речевой информации (РИ) остаются весьма актуальными. В рамках данной работы рассмотрены системы защиты РИ для современной модели связи. Такая модель является мультимодальной и многопотоковой и подразумевает наличие большого числа абонентов, которые имеют возможность использовать несколько линий связи для организации своего взаимодействия. С учетом этого проведен детальный анализ угроз конфиденциальности, целостности и доступности РИ. Рассмотрены существующие методы противодействия данным угрозам. Показано, что имеющиеся методы не обеспечивают безопасность речевых сообщений (РС) в полной мере и существует ряд новых угроз в области обеспечения целостности и доступности РИ, для которых на текущий момент решения отсутствуют или находятся на стадии разработки. Предложены собственные подходы для противодействия таким угрозам. Для обеспечения целостности РС наиболее перспективными являются методы стеганографии, в частности применение аудиомаркеров позволит однозначно аутентифицировать личность говорящего на протяжении всего сеанса связи. Для противодействия угрозам доступности РИ в части, касающейся пропускной способности канала связи и ограниченных объемов хранилищ данных РС, необходимы усовершенствование существующих и разработка новых адаптивных алгоритмов сжатия речи. При чем такие алгоритмы должны сохранять заданный уровень речевой разборчивости.
Ключевые слова: защита речевой информации, угрозы информационной безопасности, речевая разборчивость, аудиомаркер, адаптивное алгоритмы сжатия речи

Вячеслав М. Барбашов[1], Олег А. Калашников[2]
[1]Национальный исследовательский ядерный университет «МИФИ», 115409, Москва, Каширское шоссе, 31, Россия
e-mail: VMBarbashov@mephi.ru,ORCID 0000-0001-7136-415X
[2]АО«ЭНПОСПЭЛС»
115409, Москва, Каширское шоссе, 31, Россия
e-mail: oakal@spels.ru, ORCID 0000-0002-9473-9900

ФУНКЦИОНАЛЬНО-ЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДОЗОВЫХ РАДИАЦИОННЫХОТКАЗОВСФ-БЛОКОВ СИСТЕМ НА КРИСТАЛЛЕ

Аннотация: Рассмотрена методика функционально-логического моделирования дозовых радиационных отказов систем на кристалле, основанная на методе критериальных функций принадлежности. Проведен анализ возможностей данного подхода для определения работоспособности СФ-блоков и влияния на нее режимов функционирования.Исследованы особенности применения методики для моделирования дозовых радиационных отказов различных типов СФ-блоков: логических элементов, блоков и ячеек памяти, процессоров. Приведены примеры построения критериальных функций принадлежности и функций работоспособности этих СФ-блоков по различным критическим параметрам, характеризующим их отказы. Показано, что при моделировании

дозовых отказов необходимо учитывать влияние режима функционирования в процессе облучения на параметры моделей.Предложенная методика позволяет повысить достоверность оценки показателей радиационной стойкости СнК, в том числе с целью решения задач обеспечения информационной безопасности радиоэлектронной аппаратуры.

Ключевые слова: СнК, дозовые радиационные отказы, функционально-логическое моделирование.

Алексей Е. Сулавко[1], Самал С. Жумажанова[1], Алексей А. Нигрей[2], Лала Н. Закутнева[3]
[1]Омский государственный технический университет,
пр-т Мира, 11, г. Омск, 644050, Россия
e-mail: sulavich@mail.ru, ORCID 0000-0002-9029-8028
e-mail: samal_shumashanova@mail.ru, ORCID 0000-0002-6785-5201
[2]Омский государственный университет путей сообщения,
пр-т Маркса, 35, г. Омск, 644046, Россия
e-mail: nigrey.n@mail.ru, ORCID 0000-0002-8391-5374
[3]Снежинский физико-технический институт - филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»,
Комсомольская, 8, г. Снежинск, 456776, Россия
e-mail: zakytnevaln@yandex.ru, ORCID 0000-0002-0910-3618

ВЛИЯНИЕ ПСИХОФИЗИОЛОГИЧЕСКОГО СОСТОЯНИЯ ПОДПИСАНТА НА РЕЗУЛЬТАТЫ ЕГО ИДЕНТИФИКАЦИИ ПО РУКОПИСНОМУ ОБРАЗУ ЕСТЕСТВЕННЫМ И ИСКУССТВЕННЫМ ИНТЕЛЛЕКТАМИ

Аннотация. В настоящее время активно совершенствуются различные механизмы обеспечения информационной безопасности, и особое внимание уделяется предотвращению несанкционированного доступа к информационным ресурсам. Наиболее слабым звеном остается человеческий фактор и процесс идентификации, а также аутентификации пользователя. Совершенствование технологий защиты информационных ресурсов от внутренних угроз безопасности лежит на пути перехода к биометрическим системам скрытой идентификации пользователей компьютера и их психофизиологического состояния. Изменение психофизиологического состояния отражается на почерке человека. В работе проведена оценка влияния состояния утомления и возбуждения подписантов на результаты их идентификации человеком и методами распознавания образов по воспроизводимым подписям. Осуществлено сравнение возможностей естественного и искусственного интеллекта в равных условиях. При изменении состояния подписанта вероятность ошибок его распознавания искусственным интеллектом возрастает в 3,3-3,7 раз. Человек идентифицирует рукописный образ с меньшим числом ошибок, если подписант возбужден, и с большим числом ошибок, если он утомлен.

Ключевые слова: идентификационные признаки, внешний вид подписи, динамика воспроизведения рукописного пароля, алгоритм распознавания образов человеком и автоматом, формула Байеса.

Natalia G. Miloslavskaya, Alexander I. Tolstoy
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: NGMiloslavskaya@mephi.ru, ORCID 0000-0002-1231-1805
e-mail: AITolstoj@mephi.ru, ORCID 0000-0001-9265-1510

Competence Requirements of ISO/IEC Standards for Information Security Professionals

Abstract. The rapid progress in the filed of information security (IS) puts one in a need of periodic revision of professional competencies (formulated in the federal state educational standards –FSESs) and working functions (formulated in the professional standards – PSs). Under these conditions, a timely reaction to everything new that emerges or will appear in modern regulatory documents (primarily in standards) is extremely important. We make a forecast for the content of the ISO/IEC 27021 and ISO/IEC 19896 standards drafted by the International Organization for Standardization (ISO), which should contain the requirements for the competencies of IS management system professionals and the competence of IS testers and evaluators. Our forecast takes into account the requirements of the ISO/IEC 27000 standard group and the recommendations of the European e-Competence Framework e-CF 3.0.
Keywords: information security, competence, Information Security Professional, ISO/IEC standard

Nikolay S. Egoshin, Anton A. Konev, Alexander A. Shelupanov
Tomsk State University of Control Systems and Radioelectronics,
Lenin Av., 40 Tomsk, 634050, Russia
e-mail: ens@csp.tusur.ru, ORCID 0000-0003-4770-0701
e-mail: kaa@keva.tusur.ru, ORCID 0000-0002-3222-9956
e-mail: saa@keva.tusur.ru, ORCID 0000-0003-2393-6701

Building a model of infringer

Abstract. By a model of infringer one means a set of assumptions about the specific (restricted) tools of the infringer, which the latter can use to conduct attacks. The infringer model is an important part of the organization's information security. One should realize that ignoring the model, or building it without due care, can seriously affect the security of confidential information and lead to its loss. The infringer model is informal, which implies the absence of strict and unambiguous methodology for developing such a model. There exist many academic and technical publications proposing various methods of classifying violators. Meanwhile, many information security practitioners are forced to create their own normative and methodological documents, because existing models do not necessarily capture all the aspects of the organization's work. Despite the fact that many models have a high level of correlation between classification characteristics, it has not been possible to work out a unified model so far. We attempt to develop our own methodology for building the infringer model. We have started this project by outlining the roadmap: (1) study the existing methods of constructing the infringer model; (2) identify shortcomings of existing methods; (3) develop a model of the infringer and a methodology for listing the most likely violators, with taking into account the identified shortcomings. In the process of implementation of the plan, we have analyzed several existing models of infringer and revealed their shortcomings and inherent difficulties. In the developed model, causal relationships between the elements of the model and the chains of the alleged consequences have been constructed, and possible types of alleged violators have been described and ranked. As a result, our model allows one to create a more deep description of the infringer.
Keywords: model of infringer, threat model, information security, confidential information.

Victor S. Gorbatov[1], Igor Y. Zhukov[2], Oleg N. Murashov[2]
[1]*National Research Nuclear University MEPHI*
Kashirskoe shosse, 31,Moscow, 115409, Russia
e-mail: VSGorbatov@mephi.ru, ORCID 0000-0001-9998-9733
[2]*Ltd «The National Mobile Portal», Volgogradskiy pr., 2 off.36, Moscow, 109316, Russia*
e-mail: i.zhukov@inbox.ru, ORCID 0000-0002-4429-8799
e-mail: olegxozbox@yandex.ru, ORCID 0000-0002-4467-2170

Authentication and common key generation cryptographic protocol for vehicle tachographs

Abstract. We present a public key generation protocol. The key is used for subscriber authentication in tachographs installed on vehicles in order to provide traffic safety. The protocol is based on the well-known Russian cryptographic algorithms. It ensures integrity and authenticity of data transmitted through communication channel between the on-board devices and vehicle tachograph cards. The protocol was developed in accordance with the Rosstandart recommendations and complies with the development and modernization principles for data protection encryption (cryptographic) means. The protocol was suggested as a national standard draft and is open for public discussion in accordance with the established procedure.
The main results of our study is the formulation of certain security tasks identical to those used by potential infringers to compromise the protocol. This allows one to account for structural features that will ensure further protocol compliance to the target security characteristics, as well as to guarantee subsequent justification of feature set sufficiency.
Keywords: Smart Building, Management Systems, Internet of Things (IoT)

Sergey V. Zapechnikov, Polina O. Kozhukhova
National Research Nuclear University MEPhI,
Kashirskoe shosse, Moscow, 31, 114509, Russian Federation
e-mail: SVZapechnikov@mephi.ru, ORCID 0000-0002-7975-6040
e-mail: PKozhukhova@yandex.ru, ORCID 0000-0002-4004-5209

On cryptographic security of end-to-end encrypted connections in WhatsApp and Telegram messengers

Abstract. The aim of this work is to analyze the available possibilities for improving secure messaging with end-to-end connections under conditions of external violator actions and distrusted service provider. We made a comparative analysis of cryptographic security mechanisms for two widely used messengers: Telegram and WhatsApp. It was found that Telegram is based on MTProto protocol, while WhatsApp is based on the alternative Signal protocol. We examine the specific features of messengers implementation associated with random number generation on the most popular Android mobile platform. It was shown that Signal has better security properties. It is used in several other popular messengers such as TextSecure, RedPhone, GoogleAllo, FacebookMessenger, Signal along with WhatsApp. A number of possible attacks on both messengers were analyzed in details. In particular, we demonstrate that the metadata are poorly protected in both messengers. Metadata security may be one of the goals for further studies.
Keywords: cryptography, end-to-end connection, encryption, WhatsApp, Telegram

Yury E. Kozlov, Vladimir L. Evseev
Financial University under the Government of the Russian Federation (Financial University), LeningradskyProspekt, 49, Moscow, 125993, Russia
e-mail: kozlovye@yandex.ru, ORCID 0000-0002-4448-0232
e-mail: VLevseev@fa.ru, ORCID 0000-0003-3283-3106

Multimodal three-dimensional dynamic signature

Abstract. Reliable authentication in mobile applications is among the most important information security challenges. Today, we can hardly imagine a person who would not own a mobile device that connects to the Internet. Mobile devices are being used to store largeamounts of confidential information, ranging from personal photos to electronic banking tools. In 2009,colleagues from Rice University together with their collaborators from Motorola, proposed an authentication through in-air gestures. This and subsequent workcontributing tothe development of the method are reviewed in our introduction. At the moment, there exists a version of the gesture-based authentication software available for Android mobile devices. This software has not become widespread yet. One of likely reasons for that is the insufficient reliability of the method, which involvessimilar to its earlier analogsthe use of only one device. Here we discuss the authentication based on the multimodal three-dimensional dynamic signature (MTDS) performed by two independent mobile devices. The MTDS-based authentication technique is an advanced version of in-air gesture authentication. We describe the operation of a prototype of MTDS-based authentication, includingthe main implemented algorithms, as well as some preliminary results oftesting the software. We expect that our method can be used in any mobile application, provided a number of additional improvementsdiscussed in the conclusionare made.
Keywords: authentication, mobile device, accelerometer, personalized gestured, signature

Aleksandr V. Kuznetcov
Financial University under the Government of the Russian Federation(Financial University), Leningradsky prospect, 49, Moscow, 125993, Russia
e-mail: a.kuznetsov@ntc-vulkan.ru, ORCID 0000-0002-7160-1845

Software for security event management:Development and utilization

DOI: http://dx.doi.org/10.26583/bit.2017.4.06

Abstract. We address the challenge to the information security coming from the lack of algorithmic machinery for managing the security events. We start with a mathematical formulation of the problem for a tabular processor by introducing an appropriate target function. Details of corresponding algorithm can be found by following the provided links. We describe our original software module that implements the algorithm for determining the registered security events. The module is based on the tabular processor certified by the Russian Federal Service for Technical and Export Control. We present a control sample for testing the developed module. The sample has the dimension 30x20 and contains 14 choices for threshold values of security events number. The results of the tests comply with the specified boundary conditions and demonstrate a nonlinear dependence of the objective function onthe number of registered security events, as well as a nonlinear dependence of the percentage of the detected security event on the total initial number of security events to be registered at the event source. The performance of the module specifically, the central processing unit usage is found acceptable (not exceeding 33%), which allows one to use the software for typical automated workplaces equipped with appropriate tabular processors. Our approach is universal with respect to the application areas.
Keywords: security event, security event management, SIEM, event source, tabular processor.

Sergei B. Kozlachkov[1], Andrew M. Bonch-Bruevich[1], Sergey V. Dvoryankin[2]
Nadezhda V. Vasilevskaya[3], Alexandra L.Selenina[1]
[1]Bauman Moscow State Technical University, 2nd Bauman Street, 5, Moscow, 105005, Russia
e-mail: ksb.perovo@mail.ru, ORCID 0000-0002-7096-6711
e-mail: 123andryb@mail.ru, ORCID 0000-0002-4453-2979
e-mail: so.zz.va@yandex.ru,ORCID 0000-0002-4280-8214
[2]Financial University under the Government of the Russian Federatio (Financial University), LeningradskyProspect, 49, Moscow, 125993, Russia
e-mail: SVDvoryankin@fa.ru, ORCID 0000-0001-6908-0676
[3]FSTEC of Russia, Staraya Basmannaya street, 17, Moscow, 105066, Russia
e-mail: infuzoriavalenoc@yandex.ru, ORCID 0000-0002-0078-8665

Specific features of the formation of an acoustoelectric channel of speech information leakage

Abstract. We address the problem of assessing the protection level of the acoustoelectric channel of speech information with respect to leakages associated with specific operation principles of various electromechanical transducers. We analyze the scope of methodological and technical tools for the acoustical speech intelligence (ASI) with respect to corresponding technical channels of leakage of acoustic speech information (TCLSI). Special attention is paid to the regime of timed analysis of speech messages (distorted by noise and interference), allowing one to significantly improve the quality of the original audio signals. We list basic methods of noise reduction that can be used for processing the secondary signals of acoustoelectric leakage channels. We describe typical distortions that occur in the process of the acoustoelectric leakage channel formation. We examine the nature and the degree of the impact of various distortions on the measures of the speech information protection (SIP). We find the effect of the nonlinear distortions of the "upper limit" type (most typical for an acoustoelectric leakage channel) on the speech intelligibility to be in significant. Along with Pokrovsky's static model of speech signals, we consider a dynamic model based on Pirogov's phonetic function. The limitations of the static model are discussed, along with revealing the nature of the effect of the dynamic characteristics on speech intelligibility. We explain the effects of invariance with respect to linear distortions in the leakage channel. We perform an experimental study the results of which contradict, to a certain extent, the postulates of the formant theory used to assess the SIP level. We identify a number of mechanisms to improve the noise immunity of voice communications, allowing one to reconstruct speech signals (SS) distorted by noise and interference. We conclude with specifying a number of ways of improving SIP assessment methods in TCLSI.
Keywords: voice acoustic reconnaissance, acoustoelectric transducers, formants, phonemes, information protection, speech intelligibility, speech signal.

Roman A. Ustinov
Financial University under Government of the Russian Federation (Financial University), Leningradsky Prospekt, 49, Moscow, 125993, Russia
e-mail: public-ura@yandex.ru, ORCID 0000-0002-8454-9951

Specific features of modern voice protection systems

Abstract. Nowadays, speech technologies are among the most vibrant sectors of the world's economy. Of high importance is the problem of ensuring the security of speech information (SI). Here we discuss SI protection systems within a modern communication model. The model is multimodal, multithreaded, and implies a large number of subscribers interacting via several communication lines. With this in mind, we perform a detailed analysis of threats to the

confidentiality, integrity and accessibility of SI. Existing methods of counteraction against these threats are discussed, and shown to be insufficient to ensure the safety of voice messages (VM) in full. Mean while, there are new threats to the integrity and accessibility of SI, the solutions for which are either do not exist, or only being developed. We propose our original approach to counter these threats. Steganography methods are the most promising for ensuring the integrity of the VM. In particular, using audiomarkers allows one to reliably trace speaker'sidentity throughout the entire communication session. In order to counter the threats to SI availability due to the capacity of the communication channel and the limited volumes of VM data storage, it is necessary to improve existing adaptive speech compression algorithms, along with developing new ones. Furthermore, such algorithms must keep the specified level of speech intelligibility.
Keywords: protection of speech information, threats to information security, speech intelligibility, audiomarker, adaptive compression algorithms

VyacheslavM.Barbashov[1], OlegA.Kalashnikov[2]
[1]National Research Nuclear University MEPHI
Kashirskoeshosse, 31, Moscow, 115409, Russia
e-mail: VMBarbashov@mephi.ru, ORCID 0000-0001-7136-415X
[2] JSC "ENGOs SPELS",
Kashirskoeshosse, 31, Moscow, 115409, Russia
e-mail: oakal@spels.ru, ORCID 0000-0002-9473-9900

Functional-logic simulation of IP-blocks dose functional failures

Abstract. The technique of functional-logical simulation of System-on-Chip (SoC) total dose radiation failures is presented based on fuzzy logic sets theory. An analysis of the capabilities of this approach for IP-blocks radiation behavior is carried out along with the analysis of operating modes under irradiation influence on IP-blocks radiation behavior. The following elements of this technique application for simulation of dose radiation failures of various types of IP-units are studied: logical elements, memory units and cells, processors. Examples of criterial membership functions and operability functions construction are given for these IP-units and for various critical parameters characterizing their failures. It is shown that when modeling total dose failures it is necessary to take into account the influence of the functional mode on the model parameters. The technique proposed allows improving the reliability of the SoC radiation hardness estimation, also for the purpose of solving the problems of information security of electronic devices.
Keywords: SoC, total dose failures, functional-logical simulation.

Alexey E. Sulavko[1], Samal S. Shumashanova[1], Alexey A. Nigrey[2], Lala N. Zakutneva[3]
[1]Omsk state technical university, pr. Mira, 11, Omsk, 644050, Russia
e-mail: sulavich@mail.ru, ORCID 0000-0002-9029-8028
e-mail: samal_shumashanova@mail.ru, ORCID 0000-0002-6785-5201
[2]Omsk state transport university, pr. Marksa, 35, Omsk, 644046, Russia
e-mail: nigrey.n@mail.ru, ORCID 0000-0002-8391-5374
Snezhinskiy physical technical Institute-branch of federal state autonomous educational institution of higher professional education national research nuclear university "MIFI", Komsomolskaya, 8, Snezhinsk, 456776, Russia
e-mail: zakytnevaln@yandex.ru, ORCID 0000-0002-0910-3618

Influence of the signer's psychophysiological state on the results of his identification using handwritten pattern by natural and artificial intelligence*

Abstract. At present, while various mechanisms to ensure information security are actively being improved, particular attention is paid to prevent unauthorized access to information resources. The human factor and process of identification still remain the most problematic, as well as user authentication. A progress in the technology of information resources protection from internal security threats paves its way towards biometric systems of hidden identification of computer users and their psychophysiological state. A change in psychophysiological state results in the person's handwriting. The influence of the signer's state of fatigue and excitation on the results of its identification both by a person and by pattern recognition methods on reproduced signatures are studied. Capabilities of human and artificial intelligence are compared in equal conditions. When the state of the signer changes, the probability of erroneous recognition by artificial intelligence increases by factor 3.3 to 3.7. A person identifies a handwritten image with fewer errors in case when the signer is agitated, and with higher error rate if the signer is tired.
Keywords: identification features, appearance of the signature, password handwriting dynamics, pattern recognition algorithm by human and machine, Bayes' formula.

Рукописи, предоставляемые в редакцию, должны соответствовать следующим требованиям:

– тема статьи должна быть актуальной, иметь научное или практическое значение и публиковаться авторами впервые;
– рукопись должна быть оформлена только в формате *.doc, полоса А4, кегль 12, шрифт TimesNewRoman, интервал полуторный;
– в начале статьи идут сведения о статье **на английском языке**: И.О. Фамилия авторов (по центру, строчными буквами); далее сведения об авторах – должность, ученая степень, ученое звание, место работы, контактный телефон, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив); затем название статьи (по центру, строчными буквами, полужирно с подчеркиванием); ключевые слова (не более шести, по ширине, курсив); аннотация (8–12 строк, по ширине, строчными буквами);
– далее идут сведения о статье **на русском языке**: И.О. Фамилия авторов (по центру, строчными буквами); далее сведения об авторах – должность, ученая степень, ученое звание, место работы, контактный телефон, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив); затем название статьи (по центру, строчными буквами, полужирно с подчеркиванием); ключевые слова (не более шести, по ширине, курсив); аннотация (8–12 строк, по ширине, строчными буквами);
– затем идет текст статьи на русском или английском языке, кегль 12, интервал полуторный, рекомендуемый общий объем статьи не должен превышать 10 страниц, включая таблицы, иллюстрации;
– в конце статьи приводится СПИСОК ЛИТЕРАТУРЫ, в котором указан библиографический список источников литературы, оформленный в соответствии с действующими стандартами (как правило, не менее 15 наименований);
– после списка литературы идет REFERENCES, в котором эти библиографические источники должны быть написаны латиницей (т.е. латинскими буквами).

Условия опубликования статьи:

– статья может быть выслана по электронной почте или представлена в редакцию на бумажном (одном экземпляре) и электронном носителях (кроме дискет);
– редакционная коллегия журнала следует этическим нормам, принятым в международном научном сообществе, опираясь на рекомендации Комитета по этике научных публикаций, не противоречащим нормам российского законодательства в областях регулирования деятельности средств массовой информации и авторского права;
– статьи, не соответствующие установленным требованиям представления и оформления, не рассматриваются и не публикуются;
– в одном номере журнала публикуется, как правило, только одна статья автора, в том числе с соавторами;
– авторы должны предоставлять только оригинальные работы, при использовании текстовой или графической информации, полученной из работ других лиц, необходимы ссылки на соответствующие публикации или письменное разрешение автора;
– решение о публикации рукописи принимается редакционной коллегией на основании результата рецензирования и экспертной оценки квалифицированными специалистами в области ИБ;
– в случае приема рукописи к публикации автор должен оперативно давать ответы на вопросы редакции, связанные с замечаниями по статье;
– в случае отказа в публикации редакционная коллегия должна предоставить автору копию рецензии и обоснование отказа публикации;
– подача статьи в более чем один журнал одновременно расценивается как неэтичное поведение и является неприемлемой;
– статьи публикуются бесплатно.

Правила оформления текстов для публикации

1. Статьи необходимо подавать в электронном виде (*.doc или *.rtf) с распечаткой (или файлом в формате *.pdf) – во избежание неточностей прочтения формул.
2. Картинки, графики, фотографии и другие виды иллюстраций, по возможности, следует предоставлять не только включенными в текст, но и отдельными файлами в исходном формате (не интегрированными в документ Word).
3. Сокращения и аббревиатуры, которых нет в списке сокращений, необходимо раскрывать (в скобках или в сноске).
4. Давая в тексте статьи ссылки на формулы, выражения или ограничения, пожалуйста, убедитесь в том, что соответствующие объекты в статье есть и пронумерованы.
5. Ссылки на литературу следует давать в тексте в квадратных скобках, в случае цитирования – с указанием страниц.
6. При оформлении списка литературы желательно обращать внимание на наличие выходных данных работ и избегать повторных указаний одной и той же работы под разными номерами.
7. Ссылки на законы, нормативные акты, конфенции и прочее желательно указывать по установленной форме: Закон РФ «__» от х месяца хххх г. № ___. Ст. ___.
8. Иноязычные слова, термины и фамилии, написание которых допускает варианты, просьба писать в пределах одной статьи одинаково.

Заранее спасибо, редакционная коллегия

The articles submitted to the editors must meet the following requirements:

– the topic of the article should be relevant, have scientific or practical significance and be published by the authors for the first time;
– the manuscript should be formatted only in * .doc or pdf format, A4 strip, size 12, TimesNewRoman font, one-and-a-half interval;
– in the beginning of the article there are information about the article in English: I.O. Name of authors (centered, lower case); Further information about authors – position, academic degree, academic title, place of work, contact phone number, e-mail address and personal identifier ORCID (centered, lowercase, italics); Then the title of the article (centered, lowercase, bold with underline); Keywords (no more than six, in width, italics); Annotation (8–12 lines, width, lower case);
– Further information on the article is in Russian: I.O. The authors' surname (for jubilus, lower case letters); Further information about authors – position, academic degree, academic title, place of work, contact phone number, e-mail address and personal identifier ORCID (centered, lowercase, italics); Then the title of the article (centered, lowercase, bold with underline); Keywords (no more than six, in width, italics); Annotation (8–12 lines, width, lower case);
– then the text of the article is in Russian or English, size 12, interval one and a half, the recommended total volume of the article should not exceed 10 pages, including tables, illustrations;
– at the end of the article the LIST OF LITERATURE is given, in which the bibliographic list of sources of literature is indicated, drawn up in accordance with the current standards (as a rule, not less than 15 titles);
– after the list of literature is REFERENCES, in which these bibliographic sources should be written in Latin (ie Latin letters).

Terms of publication of the article:

– the article should be sent by e-mail;
– The editorial board of the journal follows the ethical standards adopted in the international scientific community, relying on the recommendations of the Ethics Committee of scientific publications that do not contradict the norms of Russian legislation in the field of regulation of the activities of the media and copyright;
– articles that do not meet the requirements for presentation and processing are not considered or published;
– in one issue of the journal, as a rule, only one author's article is published, including coauthors;
– authors should provide only original works, if text or graphic information obtained from other persons is used, references to the relevant publications or the author's written permission are necessary;
– the decision to publish the manuscript is made by the editorial board on the basis of the result of peer review and expert evaluation by qualified specialists in the field of information security;
– in the case of receipt of the manuscript for publication, the author must promptly give answers to editorial questions related to comments on the article;
– in case of refusal to publish, the editorial board should provide the author with a copy of the review and justification for refusing the publication;
– Submitting an article to more than one journal is simultaneously regarded as unethical behavior and is unacceptable;
– articles are published for free.

Rules for publication of texts

As part of the submission process, authors are required to check off their submission's compliance with all of the following items, and submissions may be returned to authors that do not adhere to these guidelines.
1. This article has not been previously published, and not submitted for review and publication in another journal (or a corresponding explanation if otherwise in the Comments to the editor).
2. File with the articles submitted in the one jf the following document format OpenOffice, Microsoft Word, RTF, or WordPerfect.
3. The full web address (URL) for links are given where it is possible.
4. The text is single-spaced; uses a font size of 12 points; to highlight use italics, not underlining (except for URL addresses); all illustrations, graphs and tables located in the appropriate places in the text, not at the end of the document.
5. The text complies with the stylistic and bibliographic the requirements described in the Guide for authors, on the «About the journal» page.
6. If you are submitting an article in a peer reviewed section of the journal then the document meets the requirements to ensure blind peer review.

Submission Preparation Checklist

As part of the submission process, authors are required to check off their submission's compliance with all of the following items, and submissions may be returned to authors that do not adhere to these guidelines.
1. This article has not been previously published, and not submitted for review and publication in another journal (or a corresponding explanation if otherwise in the Comments to the editor).
2. File with the articles submitted in the one jf the following document format OpenOffice, Microsoft Word, RTF, or WordPerfect.
3. The full web address (URL) for links are given where it is possible.
4. The text is single-spaced; uses a font size of 12 points; to highlight use italics, not underlining (except for URL addresses); all illustrations, graphs and tables located in the appropriate places in the text, not at the end of the document.
5. The text complies with the stylistic and bibliographic the requirements described in the Guide for authors, on the «About the journal» page.
6. If you are submitting an article in a peer reviewed section of the journal then the document meets the requirements to ensure blind peer review.

Privacy Statement

The names and email addresses entered in this journal site page will be used exclusively for the purposes specified by this journal and will not be used for any other purposes or will not be given over to another individuals and organizations.

АБИ – администратор безопасности информации
АнД – аналоговый документ
АРМ АБИ – автоматизированное рабочее место администратора безопасности информации
АС – автоматизированная система
БД – база данных
БИС – большая интегральная схема
ИБ – информационная безопасность
ИКТ – информационно-коммуникационные технологии
ИП – информационные продукты
ИПС – изолированная программная среда
ИР – информационные ресурсы
КСЗ – комплекс средств защиты
КТЭ – компьютерно-техническая экспертиза
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НД – нормативный документ
НСД – несанкционированный доступ
ОИ – объект информатизации
ОС – операционная система
ПАК – программно-аппаратный комплекс
ПО – программное обеспечение
ПРД – правила разграничения доступа
ПСКЗИ – персональное средство криптографической защиты информации
РД – руководящий документ
РКБ – резидентный компонент безопасности
РПВ – разрушающее программное воздействие
СВТ – средство вычислительной техники
СЗИ – средство защиты информации
СЗИ НСД – средство защиты информации от несанкционированного доступа
СКЗИ – система криптографической защиты информации
СРД – система разграничения доступа
СУБД – система управления базами данных
ЭлД – электронный документ
ЭЦП – электронная цифровая подпись

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ = IT Security.
Том 24. № 4(2017)

Адрес редакции: Каширское шоссе, 31, Москва, 115409, Россия
Тел.: +7 (495) 788 5699, тоновый режим 9216 или 9087.
Факс: +7 (499) 324-86-00.
Editorial address: Kashirskoe shosse, 31, Moscow, 115409, Russia
Tel. +7 (495) 788 5699, tone mode set 9216 or 9087.
Fax: +7 (499) 324-86-00.
E-mail: BIT@mephi.ru
https://bit.mephi.ru

Периодичность выхода - 4раза в год / Periodicity - 4 times a year

Подписка на журнал
производится на почтовых отделениях связи
по каталогу «Пресса России»

Подписной индекс 29226

Цена в продаже свободная / Price selling free

Технический редактор Т.В. Волвенкова
Корректор Е.Г. Станкевич
Верстка Г.А. Бобровой

Подписано в печать 12.12.2017. Формат 60x84 1/8.
Печ.л. 15,5. Уч.-изд.л. 15,5. Тираж 500 экз. Изд. № 009-3

Национальный исследовательский ядерный университет «МИФИ»
Каширское шоссе, 31, Москва, 115409, Россия

National Research Nuclear University MEPHI
Kashirskoe shosse, 31, Moscow, 115409, Russia

Типография ООО «Клуб печати»
127018, Москва, Марьиной Рощи 3-й проезд, 40