ISSN 2225-5435

Вестник УрФО.

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 4(38) / 2020

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство ПИ № ФС77-65765 от 20.05.2016

Издатель: **ООО «Южно-Уральский юридический вестник»**

Адрес редакции и издателя: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.
Тел./факс (351) 267-97-01.

Электронная версия журнала в Интернете:
www.info-secur.ru,
e-mail: urvest@mail.ru

16+

Journal of the Ural Federal District. Information security

ISSN 2225-5435

№ 4(38) / 2020

FOUNDER

SOUTH URAL STATE UNIVERSITY

SOUTH URAL LEGAL NEWSLETTER

CHAIRMAN OF THE EDITORIAL BOARD

CHUVARDIN O. P.,

Head of Department Federal Service for Technical and Export Control of Russia for the Urals Federal District

CHIEF EDITOR

SOKOLOV A.N.,

Ph.D., Associate Professor, Head of Department "Information Protection", South Ural State University (National Research University) (Chelyabinsk city)

PRODUCING EDITOR

SOGRIN E. K.

LAYOUT

SHRABER A. E.

PROOFREADING

FEDOROV V. S.

Subscription index 73852

in the «Russian Post» catalog

The journal is registered by the Federal service in the field of communication, information technology and mass communications.

Certificate
PI No. ФС77-65765 dd. 05/20/2016

Publisher: OOO « South Ural Legal Newsletter»

Editorial and publisher address: Russia, 454080, Chelyabinsk, Lenin Avenue, 76
Phone / fax (351) 267-97-01.

Electronic version of the magazine in the Internet:

www.info-secur.ru,
e-mail: urvest@mail.ru

16+

В НОМЕРЕ

ИССЛЕДОВАНИЕ И ПРОЕКТИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

МЕТОДЫ АНАЛИЗА ДАННЫХ

RESEARCH AND DESIGN OF TECHNICAL FACILITIES

INFORMATION TECHNOLOGY AND COMPUTER SECURITY

METHODS OF DATA ANALYSIS

УДК 004.056.5

Вестник УрФО № 4(38) / 2020, с. 5–21

Поршнев С.В., Беляев Д.О.

DOI: 10.14529/secur200401

СКРЫТЫЕ ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ: АНАЛИЗ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЙ

В процессе функционирования средств вычислительной техники (СВТ) возникают технические каналы утечки информации (ТКУИ). Сегодня перечень ТКУИ, а также методы и средства с борьбы с утечками по данным техническим каналам регламентируются действующей нормативной документа-цией в области технической защиты информации (ТЗИ). Однако оказывается, что также существует целый ряд ТКУИ, мер противодействия, которым не предусмотрено действующими нормативными документами в области ТЗИ. Для краткости данный тип ТКУИ назван скрытыми техническими каналами утечки информации (СКТУИ).

Примерами СКТУИ, используемыми для передачи данных, обрабатываемых в СВТ, являются:

– линии электропередач, в которых зависимость потребления электро-энергии от времени определяется нагрузкой центральных процессоров (CPU) СВТ, управляемых предустановленной специальной программой;

– акустический ультразвуковой канал, образованный пассивными колонками и наушниками без использования микрофона;

– низкочастотные магнитные колебания, возникающие при работе CPU СВТ;

– радиоизлучение, сопровождающее в процесс ввода информации на смартфоне, которое регистрируется и анализируется на смартфоне нарушителя с помощью FM-тюнера;

– вариаций теплового излучения корпуса СВТ;

– акустического излучения, генерируемого дисковыми накопителями в процессе записи и считывания информации;

– электромагнитного излучения, возникающего в процессе обращения к различным устройствам через порт USB;

– оптического излучения светодиодных индикаторов СВТ и т.д.

Принимая во внимание реальную опасность несанкционированного доступа к данным, обрабатываемым в СВТ, понятна необходимость научных исследований СТКУИ с

целью разработки методик оценивания угроз безопасности информации и разработки научно-обоснованных методов и средств защиты от утечки информации по данным ТКУИ.

В статье проведен обзор открытых научных публикаций, посвященных исследованиям СТКУИ, в том числе рассмотрены механизмы передачи информации по СТКУИ и экспериментальные результаты, подтверждающие работоспособность данных механизмов.

Ключевые слова: *скрытый технический канал утечки информации, средство вычислительной техники, вредоносное программное обеспечение.*

Porshnev S.V., Belyaev D.O.

REVIEW OF RESEARCH RESULTS ON HIDDEN TECHNICAL CHANNELS OF INFORMATION LEAKAGE PROCESSED BY COMPUTER TECHNOLOGY

In the process of functioning of computer equipment, technical channels of information leakage arise. Today, the list of technical channels of information leakage, as well as methods and means to combat leaks through these technical channels are regulated by the current regulatory documentation in the field of technical information protection. However, it turns out that there are also a num-ber of technical channels of information leakage, measures to counteract which are not provided for by the current regulatory documents in the field of technical information protection. For the sake of brevity, this type of technical information leakage channels is called hidden technical information leakage channels.

Examples of hidden technical channels of information leakage used to transmit data processed in a computer tool are:

– power lines in which the dependence of electricity consumption on time is determined by the load of the central processing units (CPUs) of the computer tool, controlled by a pre-installed special program;

– acoustic ultrasonic channel formed by passive speakers and headphones without using a microphone;

– low-frequency magnetic vibrations that occur during the operation of the CPU of computer equipment;

– radio emission that accompanies the process of entering information on a smartphone, which is recorded and analyzed on the intruder's smartphone using an FM tuner;

– variations of thermal radiation of the computer equipment housing;

– acoustic radiation generated by disk drives in the process of writing and reading information;

– electromagnetic radiation that occurs during access to various devices via the USB port;

– optical radiation of led indicators means of computing technology, etc.

Taking into account the real danger of unauthorized access to data pro-cessed in a computer tool, it is clear that there is a need for scientific research of hidden technical channels of

information leakage in order to develop methods for assessing threats to information security and develop scientifically based meth-ods and means of protection against information leakage using these technical channels of information leakage.

The article reviews open scientific publications devoted to the research of hidden technical channels of information leakage, including the mechanisms of information transmission through hidden technical channels of information leak-age and experimental results confirming the operability of these mechanisms.

Keywords: *hidden technical channel of information leakage, computer hardware, malicious software.*

Введение

Техническим каналом утечки информации (ТКУИ) называется совокупность источник информации (передатчик – объект разведки), линия связи (протяженная физическая среда), по которой распространяется информационный сигнал (собственно, канал передачи), а также средство приёма (пере-хвата) информации [1, 2]. Понятие «ТКУИ» оказывается неразрывно связанным с понятием «фактор, воздействующий на информацию» – «явление, действие или процесс, результатом которых являются утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней» [3]. Перечень объективных и субъективных факторов (внутренних и внешних), воздействующих на защищаемую информацию, обрабатываемую средствами вычислительной техники, которые непосредственно формируют ТКУИ выделен в [4].

Однако оказывается, что также существуют ТКУИ, наличие которых обусловлено факторами, не предусмотренных в действующих нормативно-правовых документах в области технической защиты информации (например, акустические эманации, возникающие при отображении визуальной информации на экране, параметры которых определяются законом формирования изображения [5] и др.), которые для краткости будем называть далее «скрытыми техническими каналами утечки информации» (СТКУИ). (При этом мы сознательно не даем в данной статье точного определения понятия СТКУИ, так как для это потребуется провести детальный анализ действующей отечественной и зарубежной нормативно-правой базы в области технической защиты информации, который является предметом отдельной статьи).

В статье проводится обзор открытых публикаций, в которых обсуждаются результаты исследований скрытых технических каналов утечки информации, обрабатываемой средствами вычислительной техники.

Анализ результатов изучения СТКУИ физически изолированных средств вычислительной техники

В настоящее время зарубежными специалистами в области обеспечения информационной безопасности проводятся активные исследования нерегламентированных ТКУИ, связанных с тематикой возможности извлечения информации и управления техническими средствами обработки информации с использованием скрытых технических каналов. Данный вывод подтверждает результаты информационного поиска открытых зарубежных публикаций за последние 15 лет, приведенные ниже.

1. **Цель исследования**: подтверждение гипотезы о возможности обнаружения и извлечения информации, выводимой на экран ЖК монитора, по акустическим излучениям, сопровождающим процесс отображения инфор-мации на экране ЖК монитора, с использованием тест-сигнала типа «зебра» и экранных клавиатур [5].

Результаты исследования:

– установлено, что при визуализации отдельных пикселей генерируются акустические сигналы, частоты которых зависят от цвета отдельного пикселя (например, черного или белого);

– описан механизм утечки информации, установлена зависимость формы и характеристик (частота, амплитуда) акустического сигнала от формы отображаемой информации, описаны механизмы извлечения информативной составляющей (в том числе и использованием специально разработанного приложения для смартфона) на стороне злоумышленника;

– определены источники акустического излучения в ЖК мониторе;

– доказана возможность извлечения информации о коде нажатой клавиши экранной клавиатуры из акустических сигналов, создаваемых экраном;

– для доказательства возможности распознавания символов и слов в акустическом сигнале, перехваченном по данному ТКУИ, разработано мобильное приложение, функционирующее на основе сверхточных нейронных сетей.

2. **Цель исследования**: исследование возможности регистрации сигнала, представляющего собой низкочастотное магнитное поле, генерируемое ядрами процессоров компьютера, помещенного в клетку Фарадея, па-раметры которого определяются операциями, выполняемыми ядрами про-цессоров, и извлечение информации из низкочастотного магнитного поля о выполняемых операциях [6, 7].

Результаты исследования:

– Разработана следующая модель угроз защищаемой информации:

• на атакуемом компьютере, установлено вредоносное программное обеспечение, которое собирает информацию, представляющую интерес для злоумышленника (текстовые данные, ключи шифрования, маркеры учетных данных или пароли и т.д.);

• вредоносная программа в заданное время кодирует собранную информацию, блокирует выполнение других программ и нагружает центральный процессор таким образом, что генерируется низкочастотное магнитное поле на заданной частоте, модулированное по амплитуде соответствующим бинарным сигналом, таким образом, магнитное поле оказывается носителем информации, являющейся целью нарушителя;

• на некотором удалении от компьютера установлен магнитометрический датчик, регистрирующий в установленное время магнитное поле, создаваемое компьютером;

• декодирование сигнала, зарегистрированного с выхода магнитометрического датчика.

– для реального существования предложенной модели угроз безопас-ности информации авторы разработали программу «ODINI» для стационар-ных компьютеров, а также программу «MAGNETO» для смартфонов, кото-рые могут управлять низкочастотными магнитными полями, излучаемыми зараженным вычислительными средствами за счет изменения нагрузку на ядра процессоров, при этом, не требуя специальных привилегий (например, root);

– получено экспериментальное подтверждение работоспособности исследованного ТКУИ: в заданные моменты времени были зарегистрированы сигналы с выхода магнитометрического датчика, удаленного на расстояние до 50 см от ноутбуков, до 100 см от настольных ПК и до 150 см от сервера, содержащие закодированную информацию, интересующую нарушителя;

– доказано, что клетка Фарадея в данном случае оказалась абсолютно неэффективной.

3. **Цель исследования:** подтверждение гипотезы о том, что оптическое излучение светодиодных индикаторов состояния, устанавливаемых на различных устройствах вычислительной техники, которое может быть зарегистрировано с помощью видеокамер, смартфонов и смартчасов, является ТКУИ операциях, выполняемых данным вычислительным устройством (например, светодиодная панель клавиатуры) и подтверждение гипотезы о возможности реализации вредоносного ПО, обеспечивающего передачу похищаемой информации с помощью амплитудной и частотной модуляции оптического излучения [8].

Результаты исследования:

– экспериментально обнаружена связь между характеристиками мгновенной яркости мерцания светодиодов и нажимаемой в данный момент клавишей, цифровой код которой представляет собой некоторую последовательность нулей и единиц;

– дано объяснение обнаруженному эффекту, который обусловлен тем, что в процессе передачи той или иной двоичной последовательности в процессор вычислительного устройства из-за изменения нагрузки процессора и, соответственно, потребляемой им электрической мощности, что приводит к возникновению амплитудной и частотной модуляции оптического излучения светодиодов индикаторной панели с характерным периодом несколько микросекунд, что делает их незаметным для человеческого глаза;

– экспериментально подтверждена возможность регистрации оптического излучения светодиодов клавиатуры светочувствительными датчиками, удаленными от источника излучения на расстояние до 50 метров, в том числе камерами смартфонов и смартчасов, оснащенных соответствующими светофильтрами, даже при незначительном освещении;

– продемонстрирована возможность увеличения периода амплитудной и частотной модуляции оптического излучения светодио-

дов индикаторных панелей вычислительных устройств помощью специально разработанного программного обеспечения;

– предложен алгоритм анализа параметров амплитудной и частотно-модулированной составляющих оптического излучения светодиодов индикаторных панелей вычислительных устройств, обеспечивающий идентификацию кода нажатой на клавиатуре клавиши.

4. **Цель исследования:** исследование возможности утечки информации из высокозащищенных и/или изолированных компьютерных сетей по оптическому каналу, создаваемому светодиодами, используемыми в сетевом оборудования (коммутаторами локальной сети, маршрутизаторами и т.д.) [9].

Результаты исследования:

– предложена следующая модель угроз безопасности информации:

• в изолированную компьютерную сеть внедрен вредоносный код, функционирующий в коммутаторе или маршрутизаторе локальной сети, который получил полный контроль и управление над индикаторами состояния сети;

• вредоносный программный код имеет доступ к информации, передаваемой в защищенной компьютерной сети;

• вредоносный программный код кодирует информацию, передаваемую в защищенной компьютерной сети, и использует для ее для модуляции соответствующими кодами оптического излучения индикаторов состояния сети;

• модулированное оптическое излучение индикаторов состояния сети регистрируется оптическим датчиком выбранного типа и затем декодируется.

– представлены схемы модуляции и кодирования данных, а также разработанный протокол передачи данных;

– проведен анализ двух типов атак:

• на уровне микропрограммного обеспечения, в которых вредоносное программное обеспечение устанавливается на микропрограммном уровне сетевого коммутатора или маршрутизатора;

• вредоносный программный код имеет доступ к информации, передаваемой в защищенной компьютерной сети;

• атаки на уровне программного обеспечения, в которых вредоносный код управляет светодиодами с зараженного компьютера через стандартные каналы удаленного управления (например, SSH и telnet) или используя определенных уязвимостей компьютерной сети, при этом не требуется наличие вредоносной прошивки у маршрутизатора.

5. Цель исследования: подтверждение гипотезы о возможности несанкционированного доступа к информации об операциях, выполняемых накопителями на жестких магнитных дисках (НЖМД) на основе регистрации оптического излучения светодиодных индикаторов состояния НЖМД [10].

Результаты исследования:

– результаты исследования аналогичны результатам, полученным в [8] (см. п.3).

6. **Цель исследования:** исследование возможности несанкционированного доступа к цифровой информации в процессе ее чтения с накопителей на жестких магнитных дисках записи и, соответственно, записи на основе анализа возникающих при этом акустических излучений (акустических эманаций) [11, 12].

Результаты исследования:

– проведен анализ реальных акустических сигналов, зарегистрированных в различных режимах работы НЖМД, и выявлена связь между их количественными характеристиками и выполняемыми операциями;

– для использования в научных целях разработана вредоносная программа «Disk Filtration», устанавливаемая на скомпрометированном компьютере, которая обеспечивает генерацию акустического излучения на выбранных звуковых частотах путем управления движением рычага привода жесткого диска;

– предложен возможный механизм утечки информации, в соответствие с которым перехватываемая цифровая информация используется для преобразования несущего акустического сигнала в амплитудно-манипулированный сигнал, регистрируемый ближайшим приемником (например, смартфоном, умными часами, ноутбуком и т. д.);

– предложена модель угроз безопасности информации, соответствие с которой:

• вредоносная программа, установленная на компьютере, собирает данные для извлечения (например, пароли или ключи шифрования), а затем передает их с помощью акустических сигналов, излучаемых жестким диском;

• для амплитудной модуляции акустического излучения жесткого диска вредоносная программа преднамеренно выполняет опе-

рации поиска информации на диске, которые заставляют рычаг привода жесткого диска совершать механические движения, за счет которых обеспечивается амплитудная акустического излучения;

• ближайший приемник принимает и декодирует акустический сигнал, и предоставляет доступ злоумышленнику к извлеченной информации.

7. **Цель исследования:** исследование возможности утечки аудиоинформации за счет принудительного переключения динамиков мультимедийного компьютера в режим микрофона [13].

Результаты исследования:

– разработан метод перехвата аудиоинформации, основанный на принудительном переключении динамиков мультимедийного компьютера в режим микрофона с помощью вредоносного ПО, использующего соответствующую функцию аудиочипа, и регистрацию генерируемого звукового сигнала с помощью аудиосистемы удаленного компьютера;

– подтверждена работоспособность предложенного метода несанкционированного доступа к аудиоинформации, в том числе приведены экспериментальные результаты, подтверждающие возможность перехвата в ультразвуковом диапазоне звуковых сигналов, в том числе продемонстрирована возможность перехвата аудиоинформации по исследуемому ТКУИ, компьютером, удаленным от атакуемого компьютера на расстояние до 9 м;

– установлено, что максимальная чувствительность динамиков и наушников, используемые пользователями мультимедийных компьютеров, находится в ближнем ультразвуковом диапазоне звуковых волн (от 18 кГц до 24 кГц);

– подтверждена возможность прямой передачи на расстояниях до 3 м скрытой связи между наушниками атакуемого компьютера и компьютером атакующего и передачи по данному ТКУИ аудиоинформации в ультразвуковом диапазоне.

8. Цель исследования: исследование возможности использования инфракрасного излучения для установления скрытой двусторонней связи между внутренней сетью организации и удаленным компьютеров злоумыш-ленника для реализации утечки данных из компьютерной сети передачи и проникновение в компьютерную сеть [14].

Результаты исследования:

– экспериментально подтверждена возможность реализации следующего сценария атаки, целью которой является несанкционированный доступ к информации в атакуемом компьютере:

• на атакуемом компьютере размещен вредоносный программный код, имеющий доступ к камерам видеонаблюдения, оснащенных инфракрас-ными светодиодами (IR LED), а также доступ к информации, представляющей интерес для нарушителя (конфиденциальные данные, ПИН-коды, пароли и ключи шифрования), которая далее преобразуется в двоичные коды;

• далее полученные двоичные коды используются вредоносносным ПО для модуляции оптического излучения инфракрасного диода API-видеокамеры;

• регистрация излучения инфракрасного диода API-видеокамеры, с помощью ИК-видеокамеры, используемой атакующей стороной, и декодирование двоичных кодов в смысловой вид;

– экспериментальна подтверждена возможность реализации следующего сценария атаки, целью которой является перехват управления атакуемым компьютером:

• на атакуемом компьютере размещен вредоносный программный код, имеющий доступ к камерам видеонаблюдения, оснащенных инфракрасными светодиодами (IR LED);

• атакующий компьютер, используя инфракрасные светодиоды, излучает модулированное кодами команд управления атакуемого компьютера;

• вредоносное ПО через ИК-видеокамеру атакуемого компьютера извлекает их выходного видеопотока соответствующий информационный сигнала, далее декодирует информационный сигнал и выполняет полученную команду;

– установлено, что утечка информации по исследованному ТКУИ возможна между удаленными друг от друга компьютерами на расстояниях от 10 до 100 м, при этом скорость передачи данных достигает 20 бит/сек, скорость приема данных – 100 бит/сек;

– продемонстрировано, что описанные способы атаки, названные авторами технологией «aIR-Jumper», при соответствующей модификации, может быть использована для несанкционированного доступа к «умными» дверными звонками и другими устройствам

Интернета-вещей, которые укомплектованы инфракрасными LED.

9. **Цель исследования:** исследование возможности использования силовых кабелей (кабелей электропитания) для извлечения данных [15].

Результаты исследования:

– экспериментально подтверждена возможность реализации следующего сценария атаки, целью которой является несанкционированный доступ к информации в атакуемом компьютере с помощью вредоносного ПО «PowerHammer», реализующего следующую модель утечки информации:

• целевой компьютер заражается вредоносной программой, которая регулирует уровень загрузки ресурсов процессоров, выбирая из них ядра, не занятые в данный момент пользовательскими операциями, и загружая их собственными задачами;

• в результате изменения загрузки процессоров соответствующим образом изменяется потребление энергии компьютером, при этом, организовав соответствующим образом изменения потребления электроэнергии, можно реализовать кодирование и передачу информации с атакуемого компьютера;

– при практической реализации описанной атаки предложено и измерять вариации мощности электрических сигналов, передаваемых в силовых сетях, используя для этого трансформатор тока, который имеется в свободной продаже.

10. **Цель исследования:** исследование возможности скрытой передачи информации из физически изолированных средств вычислительной техники на частотах стандарта GSM [16].

Результаты исследования:

– описана вредоносная программа «GSMem», которая может извлекать и передавать данные через воздушный зазор на частотах стандарта GSM. Для реализации алгоритма модуляции B-ASK использовался набор команд Streaming SIMD Extension (SSE), имеющийся в процессорах Intel и AMD, в качестве передатчика использовался процессов ПЭВМ и шина памя-ти;

– продемонстрировано, что вредоносное программное обеспечение на зараженном целевом компьютере модулирует и передает электромагнитные сигналы на выше упомянутых частотах, используя многоканальную архитектуру памяти для усиления передачи;

– показано, что передаваемые сигналы могут быть приняты и демодулированы рутkитом, помещенным в базовую прошивку соседнего сотового телефона;

– реализация прототипа Gamemaker, состоящего из передатчика и приемника, оценка его производительности и ограничений при использовании;

– демонстрация эффективности и осуществимости СТКУИ: эффективная дальности передачи с использованием стандартного мобильного телефона составляет 1 – 5,5 метра;

– установлено, что при использовании специального, но доступного для приобретения аппаратного приемника эффективная дальность канала связи ТКУИ достигает более 30 метров.

11. **Цель исследования:** проверка гипотезы о возможности использования акустических сигналов, возникающих при нажатии на клавиши клавиатуры средств вычислительной техники (в том числе, ноутбуков, мобиль-ных телефонов и банкоматов и т.д.) в качестве ТКУИ, по которому нарушитель может получить информацию о том, какие клавиши и в какой последовательности были нажаты пользователем [17].

Результаты исследования:

– продемонстрировано, что исследованная атака может быть эффективной, если нарушителю удается установить соответствие между кодом нажатой клавиши и спектром перехваченного акустического сигнала, используя для этого, например, соответствующим образом обученную нейронную сеть;

– построена модель акустического сигнала утечки информации, основанная на предположении о том, что амплитуды генерируемых акустических колебаний при нажатии на различные клавиши различны и проведены экспериментальные исследования, результаты которых подтвердили адекватность предложенной модели;

– продемонстрировано, что нейронная сеть, обученная на клавиатурном почерке конкретного пользователя, может решать задачи распознавания и классификации акустических сигналов, возникающих при нажатии на клавиши данной клавиатуры другим пользователем;

– установлено, что влияние стиля набора текста на клавиатуре (клавиатурного почерка) на качество классификации акустических сигналов, генерируемых при нажатии на клавиши, не значительно.

12. **Цель исследования:** экспериментальная проверка возможности реализации атаки, которая позволяет восстановить выводимый на печать текст на основе записи звука, который издает матричный принтер в процессе печати текста, с помощью акустического микрофона, установленного на расстоянии 10 см от принтера [18].

Результаты исследования:

– доказано, что при отсутствии априорных знаний о тексте, выводимом на печать, было правильно распознано около 72% напечатанных слов;

– доказано, что при наличии априорных сведений о тексте, выводимом на печать, было правильно распознано около 95 % напечатанных слов.

13. **Цель исследования:** исследование излучения в побочном электромагнитном канале устройства цифровой подписи ECDSA, использующего стандартную криптографическую библиотеку ОС Android [19].

Результаты исследования:

– доказано, что при использовании эллиптических кривых над простыми полями удается достаточно эффективно восстанавливать секретный ключ на смартфонах, функционирующих по управлением ОС Android, используя боковой (побочный) канал;

– впервые продемонстрирована возможность различения операций удвоения и сложения, выполняемых при использовании кривых Коблица. реализуемых в многоядерном процессоре с тактовой частотой более гига-герца.

14. **Цель исследования:** исследование возможности распознавания и восстановления вводимых с клавиатуры символов по акустическим сигналам, генерируемым при нажатии и возвращения клавиш в исходное положение [20].

Результаты исследования:

– выявлена связь между характеристиками акустического сигналом, генерируемого в процессе ввода текстовой информации с клавиатуры, и процессом ввода текста с клавиатуры, в том числе установлено, что характеристики акустических сигналов клавиатуры зависят от координат мест расположения клавиш, физическим расположением на клавиатуре;

– продемонстрирована возможность улучшения качества распознавания вводимой текстовой информации на основе идентификации не нажимаемых клавиш, но набираемых слов, что позволяет использовать дополнитель-но к свойствам акустического сигнала статистическую информацию о свойства языка;

– предложна модель атаки, основанная на использовании акустических сигналов, генерируемых в процессе ввода текстовой информации;

– предложен алгоритм анализа акустического сигнала утечки, основанный на совместном использовании методов ЦОС методов анализа данных;

– продемонстрирована возможность реконструкции отдельных слов, состоящих из 7-13 символов;

– обнаружено, что точность идентификации слов, состоящих более из 10 букв и более, составляет 90%.

– доказано, что факторами, определяющими успешность данного типа атаки, являются длина слова и количество одинаковых символов в слове.

15. **Цель исследования:** проверка гипотезы о возможности приема акустических сигналов, генерируемых при нажатии на клавиши клавиатуры, с помощью программного обеспечения VoIP и распознавания вводимых символов по их известным акустическим образам в условиях, когда у атакующего отсутствует какая-либо дополнительная информация об источнике акустического сигнала [21].

Результаты исследования:

– предложена модель угроз безопасности информации, соответствие с которой во время VoIP телефонного разговора между нарушителем жертвой, последний набирает на клавиатуре атакуемого устройства какой-либо текст (например, например, текст сообщения электронной почты или пароль), что сопровождается акустическими эманациями клавиатуры, автоматически регистрируемые микрофоном телефона жертвы и передающиеся на телефон атакующего по VoIP;

– обоснованы условия реализации изучаемой угрозы безопасности информации:

• наличие у злоумышленника информации о модели используемой клавиатуры и клавиатурном почерке жертвы;

• наличие у злоумышленника инструментов анализа акустических сигналов, в которых реализованы соответствующие методы, не требующие априорной информации об источнике акустического сигнала.

– продемонстрировано, что вероятность утечки информации по исследуемому ТКУИ

возрастает при увеличении числа символов набираемого жертвой текста.

16. **Цель исследования:** подтверждение гипотезы о возможности перехвата акустических сигналов, генерируемых клавиатурой компьютера во время использования программного обеспечения GnuPG, реализующего дешифровку текстов, зашифрованных с помощью алгоритма RSA, и извлече-ния из них значений 4096-битных ключей [22].

Результаты исследования:

– экспериментально подтверждена возможность перехвата исследуемых акустических сигналов с помощью обычного мобильного телефона, расположенного в непосредственной близости к целевому компьютеру, или более чувствительного микрофона, расположенного на расстоянии до 10 метров от целевого компьютера;

– продемонстрирована возможность определения полных значений 4096-битных секретных ключей RSA основе анализа перехваченных мобильным телефоном акустических сигналов, генерируемых клавиатурой компью-тера во время использования программного обеспечения в течение одного часа.

17. **Цель исследования:** доказательство возможности идентификации нажимаемых клавиш клавиатуры на основе анализа, генерируемых при этом акустических сигналов, излучениям клавиатуры, зарегистрированным с помощью микрофона мобильного телефона [23].

Результаты исследования:

– предложен метод идентификации нажимаемых клавиш клавиатуры, основанный на анализе временных задержек акустических сигналов, гарнируемых при последовательном нажатии на клавиши, а также анализе харак-теристик акустических сигналов с целью идентификации нескольких нажатий одной и той же клавиши, который не требует использования маркированных обучающих данных, а также лингвистического контекста;

– получены оценки качества идентификации нажатых клавиш на клавиатурах трех типов смартфонов, свидетельствующие о том, что точность разработанного авторами метода анализа перехваченных акустических сигналов составила 94%.

18. **Цель исследования:** исследование возможности извлечения информации из источников оптического сигнала, установленных компьютерах и стандартном сетевом оборудовании (сетевых картах, маршрутизаторах и т.д.), о реализуемых на них операциях (например, записи и чтения файлов и т.д.) [24].

Результаты исследования:

– экспериментально подтверждена возможность извлечения информации об операциях, выполняемых компьютером из оптических излучений интерфейсов WAN, расположенных на задней панели корпоративных маршрутизаторов, находящихся в сетевых стойках.

19. **Цель исследования:** исследование возможности восстановления данных на основе анализа оптического излучения светодиодных индикаторов, встроенных в технические средства обработки, хранения и передачи информации [25].

Результаты исследования:

– реализован программный компонент с использованием библиотеки OpenCV 3.0 (Itseez, 2015), который обеспечивает регистрацию оптического излучения светодиодных индикаторов, встроенных в технические средства обработки информации, идентификацию источников оптического излучения, а также анализ вариаций яркости оптических источников;

– экспериментально подтверждена возможность кодирования похищаемой информации и ее передачи по оптическому каналу, а также декодирования оптического излучения светодиодных индикаторов и сохранении далее извлеченной информации на вебсервер через мобильное соединение смартфона или компьютерную сеть;

– разработан алгоритм обнаружения и определения местоположения светодиодов, который основан на поиске различий между двумя последовательными кадрами.

20. **Цель исследования:** теоретическое исследование проблемы извлечения информации при использовании программноуправляемых скрытых каналами утечки информации [26].

Результаты исследования:

– разработана концептуальная модель перехвата информации по программноуправляемым техническим каналам, а также манипулирования информационными ресурсами специальным программным обеспечением.

21. **Цель исследования:** исследование возможности использования для несанкционированного доступа к аудиоинформации за счет использования ультразвуковых моде-

мов, установленных на мобильных устройствах связи [27].

Результаты исследования:

– продемонстрирована возможность реализации ТКУИ за счет использования ультразвукового модема мобильного устройства связи (Android), которое осуществляет принудительную регистрацию и передачу перехваченных акустических сигналов на мобильное устройство нарушителя;

– обосновано, что на расстоянии до 100 метров от источника излучения вероятность перехвата информации составляет 0,9–1.

22. **Цель исследования:** исследование возможности утечки звуковой информации при несанкционированном доступе к звуковой карте компьютера, находящегося в компьютерной сети [28].

Результаты исследования:

– продемонстрирована возможность перехвата аудиоинформации с помощью штатных средств звукозаписи и звуковоспроизведения персонального компьютера типа ноутбук (возможность перехвата аудиоинформации с помощью звуковой карты стационарного компьютера подтверждена в [29]).

23. **Цель исследования:** проверка гипотезы о возможности использования теплового излучения систем отопления, вентиляции и кондиционирования, подключенных к сети Интернет, для получения управления над изолированной корпоративной компьютерной сетью [30].

Результаты исследования:

– экспериментально подтверждена возможность реализации следующего сценария атаки, целью которой является несанкционированный доступ к информации в атакуемом компьютере:

• имеется изолированная корпоративная компьютерная сеть, зараженная вредоносным ПО;

• вредоносное ПО получило права управления хостами корпоративной компьютерной сети, а также права доступа к установленным в каждом компьютере тепловых датчиках, предназначенных для измерения температуры центрального процессора и передачи ее значений в BIOS;

• вредоносное ПО перехватило управление датчиками температуры и перевело их в режим измерения температуры окружающего воздуха;

• параллельно корпоративной компьютерной сети организации, охватывающей здание, в здании имеется система отопления, вентиляции и кондиционирования (HVAC), чей центр управления имеет выход в Интернет;

• злоумышленники реализовали успешную атаку и получили доступ к управлению системой HVAC;

• используя доступ к управлению системой HVAC, злоумышленник реализует изменение температуры воздуха в выбранном помещении в соответствие с кодами команды, передаваемой вредоносному ПО по тепловому каналу;

• вредоносное ПО получает сигнал с выхода теплового датчика, находящегося под его управлением, и далее, декодировав полученное сообщение, получает переданную злоумышленником команду.

– для подтверждения работоспособности обсуждаемого сценария атаки создано вредоносное программное обеспечение «HVACKer», предназначенное в том числе, для перехвата управления тепловыми датчиками, установленных в средствах вычислительной техники и их переключения в режим измерения температуры окружающей среды и разработан соответствующий line-encoding протокол, который позволяет передавать команды посредством изменения температуры;

– получены оценки скорости передачи данных по тепловому каналу, составляющие $\approx$ 40 бит/сек, что оказывается вполне достаточно для управления внедренным кодом;

– установлено, что ПО «HVACKer» можно использовать только для передачи команд в зараженную компьютерную сеть, но не для извлечения для извлечения из нее информации, так как точность тепловых датчиков, используемых в HVAC-устройствах, оказывается недостаточной для декодирования информации, передаваемой по тепловому каналу из компьютерной сети нарушителю.

24. **Цель исследования:** исследование возможности восстановления текста, набираемого на клавиатуре, основанного анализе на видеозаписи процесса набора текста пользователем. Разработка методов для отслеживания движения рук пользователей, реконструкции предложений и исправления ошибок, т.е. автоматическое восстановление текста, набранного пользователем, начинающееся с видеозаписи сеанса набора текста [31].

Результаты исследования:

– разработан программный инструмент, обеспечивающий автоматическое отслежи-

вание на видеозаписях процесса набора текста движений рук пользователей и восстановление набираемого текста, («ClearShot»), и прове-дено его тестирование в условиях близких к реальным;

– экспериментально подтверждена возможность реконструкции значительную часть набранного текста с помощью («ClearShot»);

– разработан алгоритм анализа результатов функционирования инструмента в типичной офисной среде, состоящий из двух этапов:

• 1 этап – анализ видеоинформации, записанной камерой с использованием методов компьютерного зрения (для каждого кадра видео компьютерный анализ зрения вычисляет набор клавиш, которые, вероятно, были нажаты, набор клавиш, которые, безусловно, не были нажаты, и положение пробелов);

• 2 этап – анализ и корректировка введенного текста с помощью языковых и контекстно-зависимых методов.

– в качестве доказательства работоспособности исследуемого метода представлен реконструированный текст, где каждое его слово представлено списком возможных слов-кандидатов, ранжированных по вероятности.

25. **Цель исследования:** получение оценки пропускной способности скрытых тепловых каналов утечки информации [32].

Результаты исследования:

– предложен эмпирический метод оценивания реальных (и ранее неизвестных) мощностей тепловых СТКУИ;

– обнаружено (на примерах сценариев с различными промежуточны-ми хостами и различными уровнями температурной индукции и шума), что скорость передачи информации в исследуемом канале может достигать ≈ 20,5 бит/час;

– установлено, что пропускная способность канала уменьшается почти вдвое (до 10,3 бит/час) при повышении уровня шума или более эффективном охлаждении на промежуточном хосте компьютерной сети.

26. **Цель исследования:** исследование возможности использования бытовых роботов-пылесосов в качестве средств акустической речевой разведки за счет перепрофилирования встроенных лазерных датчиков (лидаров) в систему дистанционного зондирования бытовых предметов, выступающих в роли источников вибрационных сигналов [33].

Результаты исследования:

– представлен программно-аппаратный механизм «LidarPhone», перепрофилирующий встроенный в робот-пылесос лидар в лазерный микрофон, который может воспринимать звуки от тонких вибраций, индуцированных на близлежащих объектах;

– модель угроз для данного вида атак схожа с моделью угроз, реализуемой с использованием систем дистанционного лазерного зондирования поверхностей остекления оконных проемов, за исключением того, что технология LidarPhone использует для записи отраженных сигналов внутреннюю память бытового устройства.

– установлено, что время функционирования разработанной технологии составляет порядка 19 часов непрерывного времени;

– продемонстрировано, что в условиях применения методов глубокого обучения с использованием сверточных нейронных сетей разработанная технология достигает точности классификации и распознавания акустических образов информативных символов порядка 90%, произнесенных в течение 10-20 секунд на расстоянии порядка 20 см;

– установлено, что значительными ограничивающими факторами эффективной реализации приведенной атаки являются уровень акустического давления, создаваемого в точке перехвата, и расстояние от источника сигнала до приемника, как следствие, влияющие на значение отношения «сигнал/шум».

27. **Цель исследования:** проверка гипотезы о возможности использования сенсорных датчиков технических средств интернет-вещей (IoT) в качестве устройств перехвата и восстановления акустической речевой информации [34].

Результаты исследования:

– представлен механизм «PitchIn», реализующий перехват и восстановление акустических сигналов с точностью порядка 79% от различных устройств со встроенными датчиками акселерометрного, гироскопического и микрофонного типа, расположенным на расстоянии до 1,5 метров от источника речи;

– также, как и в исследовании, приведенном в п.26, установлено, что значительными ограничивающими факторами эффективной реализации приведенной атаки являются уровень акустического давления, создаваемого в точке перехвата, и расстояние от источника сигнала до приемника, как следствие, влияющие на значение отношения «сигнал/шум».

28. **Цель исследования:** исследование возможности использования гироскопа современного смартфона в качестве средства перехвата акустической информации [35].

Результаты исследования:

– представлено разработанное мобильное приложение «Gyrophone», использующее обработку сигналов, воздействующих на гироскоп смартфона, и машинное обучение для идентификации информации говорящего и для анализа речи;

– показано, что гироскопы достаточно чувствительны для измерения акустических колебаний. Это приводит к возможности восстановления речи по показаниям гироскопа, а именно к использованию гироскопа в качестве микрофона;

– показано, что частота дискретизации гироскопа достигает 200 Гц, что охватывает часть слышимого диапазона. Это повышает вероятность подслушивания речи в непосредственной близости от телефона без доступа к реальному микрофону;

– установлено, что, поскольку частота дискретизации гироскопа ограничена, невозможно полностью восстановить перехваченную речь по измерениям одного гироскопа. Поэтому в случае использования гироскопа в качестве скрытого устройства перехвата информации необходимо прибегать к автоматическому распознаванию речи путем машинного обучения;

– показано, что в случае ограничения небольшим словарным запасом, состоящим исключительно из цифровых произношений ("один", "два", "три",...) возможно достижение успеха распознавания речи порядка 65%;

– показано, что при комбинации сигналов от двух или более смартфонов возможно увеличение эффективной частоты дискретизации акустического сигнала, при этом злоумышленник достигает более высокой скорости распознавания речи и более высокого процента (77%) успешного распозна-вания речевого контента.

29. **Цель исследования:** исследование возможности использования виброгенератора мобильного телефона в качестве микрофона [36].

Результаты исследования:

– представлено программное средство «VibraPhone», реализованное посредством преобразования механических колебаний, возникающих при воздействии акустического сигнала на виброгенератор (вибромотор) смартфона, и позволяющее использовать методы машинного обучения для распознавания информативных символов;

– установлено, что средняя точность распознавания речи составляет порядка 88% при условии расположения источника акустического сигнала на расстоянии 2 метров от смартфона и воспроизведении акустической информации при интегральном звуковом давлении 80 дБ;

– установлено, что при снижении уровня звукового давления с 80 до 60 дБ процент распознанной речи падает до 60%.

30. **Цель исследования:** исследование возможности извлечения акустической информации из параметров радиосигнала, изменяющихся за счет вибраций акустических излучателей (колонки, громкоговорители и т.д.), которые механически воздействуют на радиосигнал или на расположенные в непосредственной близости радиопередатчики [37].

Результаты исследования:

– установлено, что модель угроз, представленная в данном виде атак, концептуально схожа с механизмом, лежащем в основе лазерного радара (LADAR), который обычно используется для проверки устойчивости строительных конструкций;

– смоделирована процедура возмущения радиоволн звуковыми колебаниями: в качестве модели процесс воздействия механических колебаний на электромагнитные колебания рассмотрен как процедура низкоскоростной амплитудно-фазовой модуляции;

– с помощью разработанной модели спроектирован демодулятор в частотной области, изолирующий несущественные компоненты радиосигнала и позволяющий экстраполировать звуковые сигналы, проецировать их во временную область, которая в конечном итоге становится воспринимаемой злоумышленником;

– установлено, что в случае приема радиосигнала на фоне шумов при пиковом отношении «сигнал/шум» превышающем 15 дБ, тестеры обычно могут распознавать контент с точностью, близкой к 100%. Данное условие достигается при наблюдении радиосигнала на расстоянии от 2 до 4 метров от его источника (при этом источник радиосигнала – радиопередатчик – расположен на расстоянии до 1 метра от вибрирующего технического средства звуковоспроизведения);

– показано, что нижний СВЧ-диапазон (в

экспериментах использовали Wi-Fi – передатчики) обеспечивает более высокое значение пикового отношения «сигнал/шум» в задаче восстановления звука, колеблющееся в диапазоне от 7 до 9 дБ в экспериментах со звукоизолирующей стеной или звуконепроницаемым окном между передатчиком и приемником;

– установлено, что большие габариты устройства звуковоспроизведения обеспечивает более высокое значение пикового отношения «сигнал/шум» ввиду большего коэффициента вибрации.

Заключение

Проведенный анализ открытых публикаций, посвященных анализу результатов исследования СТКУИ, позволяет сделать следующие выводы.

1. Для создания СКТУИ и получения доступа к информации обрабатываемой средствами вычислительной техники, нарушитель может использовать тепловые, акустические и электромагнитные поля, а также внедренное в процессе эксплуатации или предустановленное специальное программное обеспечение на объекте вычислительной техники, которое не распознается программно-аппаратными средствами как вредоносное ПО, используя для этого, например, методы социальной инженерии, методы программного скрытия кода и иные известные методы.

2. Необходимо отметить высокую активность зарубежных ученых в исследованиях СТКУИ, в которых для получения доступа к информации, обрабатываемой средствами вычислительной техники, используются физические поля различной природы.

3. Принимая во внимании непрерывное совершенствование методов и средств защиты информации, средств вычислительной техники от утечки по «классическим» ТКУИ, требуется проведение целенаправленных отечественных исследований СКТУИ с целью выявления новых механизмов утечки информации по данным каналам, разработки моделей атак, адекватных методов и средств противодействия утечкам информации по СТКУИ, а также разработки соответствующей нормативно-правовой и методической базы по противодействию данным СТКУИ и проведения независимой проверки ре-зультатов зарубежных ученых с целью выявления возможных фактов использования открытых научных журналов с целью дезинформации.

Литература

1. Бузов Г.А. Защита информации ограниченного доступа от утеч-ки по техническим каналам: Справочное пособие / Бузов Г.А. – М.: Горячая линия-Телеком, 2015.

2. Зайцев, А. П. Технические средства и методы защиты информа-ции. Учебник для вузов – 7-е изд., испр. / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая Линия–Телеком, 2018.

3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

4. ГОСТ Р 51275-2006. Защита информации. Объект информатиза-ции. Факторы, воздействующие на информацию. Общие положения.

5. Daniel Genkin, Mihir Pattani, Roei Schuster, Eran Tromer. Synesthe-sia: Detecting Screen Content via Remote Acoustic Side Channels. 2019 IEEE Symposium on Security and Privacy (SP), 2019. P. 853-869. – URL: https://ieeexplore.ieee.org/abstract/document/8835386 – (дата обращения: 15.10.2019).

6. Mordechai Guri, Boris Zadov, Andrey Daidakulov, Yuval Elovici. ODINI: Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields. IEEE Transactions on Information Forensics and Security, 2019. P. 1190-1203. – URL: https://ieeexplore.ieee.org/abstract/document/8820015 – (дата обращения: 18.10.2019).

7. Mordechai Guri, Andrey Daidakulov, Yuval Elovici. MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields. February 7, 2018 – URL: https://arxiv.org/abs/1802.02317 – (дата обращения: 21.10.2019).

8. Mordechai Guri, Boris Zadov, Dima Bykhovsky, Yuval Elovici. CTRL-ALT-LED: Leaking Data from Air-Gapped Computers via Keyboard LEDs. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), 2019. P. 801-810. – URL: https://ieeexplore.ieee.org/abstract/document/8754078 – (дата обращения: 12.02.2020).

9. Mordechai Guri, Boris Zadov, Andrey Daidakulov, Yuval Elovici. xLED: Covert Data Exfiltration from Air-Gapped Networks via Switch and Router LEDs. 2018 16th Annual Conference on Privacy, Security and Trust (PST), 2018. P. 1-12.

10. Mordechai Guri, Boris Zadov, Yuval Elovici. LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED. DIMVA 2017. Detection of Intrusions and Malware, and

Vulnerability Assess-ment - 14th International Conference, 2017. P. 161-184. – URL: https://arxiv.org/ftp/arxiv/papers/1702/1702.06715.pdf – (дата обращения: 24.04.2020).

11. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise. arXiv preprint arXiv:1608.03431, 2016. – URL: https://arxiv.org/ftp/arxiv/papers/1608/1608.03431.pdf – (дата обращения: 27.03.2020).

12. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. Fansmitter: Acoustic data exfiltration from (speakerless) air-gapped computers. arXiv preprint arXiv:1606.05915, 2016. – URL: https://arxiv.org/ftp/arxiv/papers/1606/1606.05915.pdf – (дата обращения: 19.03.2020).

13. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. MOSQUITO: Covert Ultrasonic Transmissions Between Two Air-Gapped Com-puters Using Speaker-To-Speaker Communication. 2018 IEEE Conference on Dependable and Secure Computing (DSC), 2018. P. 1-8. – URL: https://ieeexplore.ieee.org/abstract/document/8625124 – (дата обращения: 15.05.2020).

14. Mordechai Guri, Dima Bykhovsky, Yuval Elovici. aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR). Computers & Security, vol. 82. P. 15-29. – URL: https://arxiv.org/ftp/arxiv/papers/1709/1709.05742.pdf – (дата обращения: 11.05.2020).

15. Mordechai Guri, Boris Zadov, Dima Bykhovsky, Yuval Elovici. PowerHammer: Exfiltrating data from air-gapped computers through power lines. IEEE Transactions on Information Forensics and Security, vol 15, 2019. P. 1879-1890. – URL: https://arxiv.org/pdf/1804.04014.pdf – (дата обращения: 26.04.2019).

16. Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, Yuval Elovici. GSMem: Data Exfiltration from Air-Gapped Computers over {GSM} Frequencies. 24th {USENIX} Security Symposium ({USENIX} Se-curity 15), 2015. P. 849-864. – URL: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-guri.pdf – (дата обращения: 08.07.2020).

17. Dmitri Asonov, Rakesh Agrawal. Keyboard Acoustic Emanations. IEEE Symposium on Security and Privacy, 2004. – URL: https://ieeexplore.ieee.org/abstract/document/1301311 – (дата обращения: 17.09.2020).

18. Michael Backes, Markus Dürmuth, Sebastian Gerling, Manfred Pinkal, Caroline Sporleder. Acoustic Side-Channel Attacks on Printers. USENIX Security symposium, 2010. P. 307-322. – URL: https://www.usenix.org/legacy/event/sec10/tech/full_papers/Backes.pdf – (дата обращения: 18.09.2020).

19. Pierre Belgarric, Pierre-Alain Fouque, Gilles Macario-Rat, Mehdi Ti-bouchi. Side-channel analysis of Weierstrass and Koblitz curve ECDSA on An-droid smartphones. Cryptographers'Track at the RSA Conference, 2016. P. 236-252. – URL: https://eprint.iacr.org/2016/231.pdf – (дата обращения: 03.09.2020).

20. Yigael Berger, Avishai Wool, Arie Yeredor. Dictionary attacks using keyboard acoustic emanations. Proceedings of the 13th ACM conference on Computer and communications security, 2006. P. 245-254.

21. Alber to Compagno, Mauro Conti, Daniele Lain, Gene Tsudik. Don't Skype & Type! Acoustic Eavesdropping in Voice-Over-IP. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 2017. P. 703-715. – URL: https://arxiv.org/pdf/1609.09359.pdf – (дата обращения: 16.09.2020).

22. Daniel Genkin, Adi Shamir, and Eran Tromer. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. Advances in Cryptology–CRYPTO 2014, 2014. P. 444-461

23. Jian Liu, Yan Wang, Gorkem Kar, Yingying Chen, Jie Yang, Marco Gruteser. Snooping Keystrokes with mm-level Audio Ranging on a Single Phone. Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, 2015. P. 142-154.

24. Joe Loughry. Optical TEMPEST. 2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE), 2018. P. 172-177. – URL: https://arxiv.org/pdf/1808.07175.pdf – (дата обращения: 21.09.2020).

25. Arthur Costa Lopes, Diego F Aranha. Platform-agnostic Low-intrusion Optical Data Exfiltration. 3rd International Conference on Information Systems Security and Privacy (ICISSP), 2017. P. 474-480. – URL: https://www.scitepress.org/Papers/2017/62115/62115.pdf – (дата обращения: 27.09.2020).

26. J.-P. Power: Mind the gap: are air-gapped systems safe from breach-es? Symantec. 2015. – URL: http://www.symantec.com/connect/blogs/mind-gap-are-air-gapped-systems-safe-breache – (дата обращения: 09.09.2020).

27. Luke Deshotels. Inaudible Sound as a Covert Channel in Mobile De-vices. 8th USENIX Workshop on Offensive Technologies (WOOT 14), 2014. – URL: https://www.usenix.org/system/files/conference/woot14/woot14-deshotels.pdf – (дата обращения: 09.09.2020).

28. Michael Hanspach, Michael Goetz. On Covert Acoustical Mesh Net-works in Air. Journal of Communications, vol. 8, no. 11. P. 758-767, 2013. – URL: https://arxiv.org/abs/1406.1213 – (дата обращения: 10.10.2020).

29. Беляев, Д.О., Волчков, Д.Н., Поршнев, С.В. О возможности ис-пользования персонального ком-

пьютера как устройства несанкционирован-ного доступа к речевой информации. 2019, В : Вестник УрФО. Безопасность в информационной сфере. 3 (33), стр. 5-11.

30. Yisroel Mirsky, Mordechai Guri, Yuval Elovici. HVACKer: Bridging the Air-Gap by Attacking the Air Conditioning System. arXiv preprint arXiv:1703.10454, 2017 – URL: https://arxiv.org/ftp/arxiv/papers/1703/1703.10454.pdf – (дата обращения: 11.05.2020).

31. Davide Balzarotti, Marco Cova, Giovanni Vigna. Clearshot: Eaves-dropping on keyboard input from video. 2008 IEEE Symposium on Security and Privacy (sp 2008), 2008. P. 170-183. – URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.413.9871&rep=rep1&type=pdf – (дата обращения: 20.10.2020).

32. Sebastian Zander, Philip Branch, Grenville Armitage. Capacity of temperature-based covert channels. IEEE communications letters, vol 15. P. 82-84. – URL: https://researchrepository.murdoch.edu.au/id/eprint/34937/1/capacity.pdf – (дата обращения: 17.09.2020).

33. .Sriram Sami, Sean Rui, Xiang Tan, Yimin Dai, Nirupam Roy, Jun Han. LidarPhone: acoustic eavesdropping using a lidar sensor. Proceedings of the 18th ACM Conference on Embedded Networked Sensor Systems, 2020. P. 701-702 – URL: www.cs.umd.edu/~nirupam/images/2_publication/posters_demo/writeup /LidarPhone_poster_SenSys20_nirupam.pdf – (дата обращения: 23.11.2020).

34. Jun Han, Albert Jin Chung, and Patrick Tague. PitchIn: eavesdrop-ping via intelligible speech reconstruction using non-acoustic sensor fusion. Pro-ceedings of the 16th ACM/IEEE International Conference on Information Pro-cessing in Sensor Networks, 2017. P. 181-192. – URL: https: //doi.org/10.1145/3055031.3055088 – (дата обращения: 25.11.2020).

35. Yan Michalevsky, Dan Boneh, and Gabi Nakibly. Gyrophone: Rec-ognizing Speech from Gyroscope Signals. 23rd USENIX Security Symposium (USENIX Security 14), 2014. P. 1053-1067.

36. Nirupam Roy and Romit Roy Choudhury. Listening through a Vibra-tion Motor. Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services, 2016. P. 57-69. – URL: https://doi.org/10.1145/2906388.2906415 – (дата обращения: 30.11.2020).

37. Teng Wei, Shu Wang, Anfu Zhou, and Xinyu Zhang. Acoustic eaves-dropping through wireless vibrometry. Proceedings of the 21st Annual Interna-tional Conference on Mobile Computing and Networking, 2015. P. 130-141.

References

1. Buzov G. A. Zashchita informacii ogranichennogo dostupa ot utechki po tekhnicheskim kanalam: Spravochnoe posobie / Buzov G.A. – M.: Goryachaya liniya-Telekom, 2015.

2. Zajcev, A. P. Tekhnicheskie sredstva i metody zashchity informacii. Uchebnik dlya vuzov – 7-e izd., ispr. / A.P. Zajcev, R.V. Meshcheryakov, A.A. SHelu-panov. – M.: Goryachaya Liniya–Telekom, 2018.

3. GOST R 50922-2006. Zashchita informacii. Osnovnye terminy i op-redeleniya.

4. OST R 51275-2006. Zashchita informacii. Ob'ekt informatizacii. Faktory, vozdejstvuyushchie na informaciyu. Obshchie polozheniya.

5. Daniel Genkin, Mihir Pattani, Roei Schuster, Eran Tromer. Synesthe-sia: Detecting Screen Content via Remote Acoustic Side Channels. 2019 IEEE Symposium on Security and Privacy (SP), 2019. P. 853-869. – URL: https://ieeexplore.ieee.org/abstract/document/8835386 – (data obrashheniya: 15.10.2019).

6. Mordechai Guri, Boris Zadov, Andrey Daidakulov, Yuval Elovici. ODINI: Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields. IEEE Transactions on Information Forensics and Security, 2019. P. 1190-1203. – URL: https://ieeexplore.ieee.org/abstract/document/8820015 – (data obrashheniya: 18.10.2019).

7. Mordechai Guri, Andrey Daidakulov, Yuval Elovici. MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields. February 7, 2018 – URL: https://arxiv.org/abs/1802.02317 – (data obrashheniya: 21.10.2019).

8. Mordechai Guri, Boris Zadov, Dima Bykhovsky, Yuval Elovici. CTRL-ALT-LED: Leaking Data from Air-Gapped Computers via Keyboard LEDs. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), 2019. P. 801-810. – URL: https://ieeexplore.ieee.org/abstract/document/8754078 – (data obrashheniya: 12.02.2020).

9. Mordechai Guri, Boris Zadov, Andrey Daidakulov, Yuval Elovici. xLED: Covert Data Exfiltration from Air-Gapped Networks via Switch and Router LEDs. 2018 16th Annual Conference on Privacy, Security and Trust (PST), 2018. P. 1-12.

10. Mordechai Guri, Boris Zadov, Yuval Elovici. LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED. DIMVA 2017. Detection of Intrusions and Malware, and Vulnerability Assess-ment - 14th International Conference, 2017. P. 161-184. – URL: https://arxiv.org/ftp/arxiv/papers/1702/1702.06715.pdf – (data obrashheniya: 24.04.2020).

11. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. DiskFiltration: Data Exfiltration

from Speakerless Air-Gapped Computers via Covert Hard Drive Noise. arXiv preprint arXiv:1608.03431, 2016. – URL: https://arxiv.org/ftp/arxiv/papers/1608/1608.03431.pdf – (data obrashheniya: 27.03.2020).

12. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. Fansmitter: Acoustic data exfiltration from (speakerless) air-gapped computers. arXiv preprint arXiv:1606.05915, 2016. – URL: https://arxiv.org/ftp/arxiv/papers/1606/1606.05915.pdf – (data obrashheniya: 19.03.2020).

13. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. MOSQUITO: Covert Ultrasonic Transmissions Between Two Air-Gapped Com-puters Using Speaker-To-Speaker Communication. 2018 IEEE Conference on Dependable and Secure Computing (DSC), 2018. P. 1-8. – URL: https://ieeexplore.ieee.org/abstract/document/8625124 – (data obrashheniya: 15.05.2020).

14. Mordechai Guri, Dima Bykhovsky, Yuval Elovici. aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR). Computers & Security, vol. 82. P. 15-29. – URL: https://arxiv.org/ftp/arxiv/papers/1709/1709.05742.pdf – (data obrashheniya: 11.05.2020).

15. Mordechai Guri, Boris Zadov, Dima Bykhovsky, Yuval Elovici. PowerHammer: Exfiltrating data from air-gapped computers through power lines. IEEE Transactions on Information Forensics and Security, vol 15, 2019. P. 1879-1890. – URL: https://arxiv.org/pdf/1804.04014.pdf – (data obrashheniya: 26.04.2019).

16. Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, Yuval Elovici. GSMem: Data Exfiltration from Air-Gapped Computers over {GSM} Frequencies. 24th {USENIX} Security Symposium ({USENIX} Se-curity 15), 2015. P. 849-864. – URL: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-guri.pdf – (data obrashheniya: 08.07.2020).

17. Dmitri Asonov, Rakesh Agrawal. Keyboard Acoustic Emanations. IEEE Symposium on Security and Privacy, 2004. – URL: https://ieeexplore.ieee.org/abstract/document/1301311 – (data obrashheniya: 17.09.2020).

18. Michael Backes, Markus Dürmuth, Sebastian Gerling, Manfred Pinkal, Caroline Sporleder. Acoustic Side-Channel Attacks on Printers. USENIX Security symposium, 2010. P. 307-322. – URL: https://www.usenix.org/legacy/event/sec10/tech/full_papers/Backes.pdf – (data obrashheniya: 18.09.2020).

19. Pierre Belgarric, Pierre-Alain Fouque, Gilles Macario-Rat, Mehdi Ti-bouchi. Side-channel analysis of Weierstrass and Koblitz curve ECDSA on An-droid smartphones. Cryptographers'Track at the RSA Conference, 2016. P. 236-252. – URL: https://eprint.iacr.org/2016/231.pdf – (data obrashheniya: 03.09.2020).

20. Yigael Berger, Avishai Wool, Arie Yeredor. Dictionary attacks using keyboard acoustic emanations. Proceedings of the 13th ACM conference on Computer and communications security, 2006. P. 245-254.

21. Alber to Compagno, Mauro Conti, Daniele Lain, Gene Tsudik. Don't Skype & Type! Acoustic Eavesdropping in Voice-Over-IP. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 2017. P. 703-715. – URL: https://arxiv.org/pdf/1609.09359.pdf – (data obrashheniya: 16.09.2020).

22. Daniel Genkin, Adi Shamir, and Eran Tromer. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. Advances in Cryptology–CRYPTO 2014, 2014. P. 444-461

23. Jian Liu, Yan Wang, Gorkem Kar, Yingying Chen, Jie Yang, Marco Gruteser. Snooping Keystrokes with mm-level Audio Ranging on a Single Phone. Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, 2015. P. 142-154.

24. Joe Loughry. Optical TEMPEST. 2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE), 2018. P. 172-177. – URL: https://arxiv.org/pdf/1808.07175.pdf – (data obrashheniya: 21.09.2020).

25. Arthur Costa Lopes, Diego F Aranha. Platform-agnostic Low-intrusion Optical Data Exfiltration. 3rd International Conference on Information Systems Security and Privacy (ICISSP), 2017. P. 474-480. – URL: https://www.scitepress.org/Papers/2017/62115/62115.pdf – (data obrashheniya: 27.09.2020).

26. J.-P. Power: Mind the gap: are air-gapped systems safe from breach-es? Symantec. 2015. – URL: http://www.symantec.com/connect/blogs/mind-gap-are-air-gapped-systems-safe-breache – (data obrashheniya: 09.09.2020).

27. Luke Deshotels. Inaudible Sound as a Covert Channel in Mobile De-vices. 8th USENIX Workshop on Offensive Technologies (WOOT 14), 2014. – URL: https://www.usenix.org/system/files/conference/woot14/woot14-deshotels.pdf – (data obrashheniya: 09.09.2020).

28. Michael Hanspach, Michael Goetz. On Covert Acoustical Mesh Net-works in Air. Journal of Communications, vol. 8, no. 11. P. 758-767, 2013. – URL: https://arxiv.org/abs/1406.1213 – (data obrashheniya: 10.10.2020).

29. Belyaev, D.O., Volchkov, D.N., Porshnev, S.V. O vozmozhnosti ispol'-zovaniya personal'nogo komp'yutera kak ustrojstva nesankcionirovannogo dostupa k rechevoj informacii. 2019, V : Vestnik UrFO. Bezopasnost' v infor-macionnoj sfere. 3 (33), str. 5-11.

30. Yisroel Mirsky, Mordechai Guri, Yuval Elovici. HVACKer: Bridging the Air-Gap by Attacking the Air

Conditioning System. arXiv preprint arXiv:1703.10454, 2017 – URL: https://arxiv.org/ftp/arxiv/papers/1703/1703.10454.pdf – (data obrashheniya: 11.05.2020).

31. Davide Balzarotti, Marco Cova, Giovanni Vigna. Clearshot: Eaves-dropping on keyboard input from video. 2008 IEEE Symposium on Security and Privacy (sp 2008), 2008. P. 170-183. – URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.413.9871&rep=rep1&type=pdf – (data obrashheniya: 20.10.2020).

32. Sebastian Zander, Philip Branch, Grenville Armitage. Capacity of temperature-based covert channels. IEEE communications letters, vol 15. P. 82-84. – URL: https://researchrepository.murdoch.edu.au/id/eprint/34937/1/capacity.pdf – (data obrashheniya: 17.09.2020).

33. Sriram Sami, Sean Rui, Xiang Tan, Yimin Dai, Nirupam Roy, Jun Han. LidarPhone: acoustic eavesdropping using a lidar sensor. Proceedings of the 18th ACM Conference on Embedded Networked Sensor Systems, 2020. P. 701-702 – URL: www.cs.umd.edu/~nirupam/images/2_publication/posters_demo/writeup /LidarPhone_poster_SenSys20_nirupam.pdf – (data obrashheniya: 23.11.2020).

34. Jun Han, Albert Jin Chung, and Patrick Tague. PitchIn: eavesdrop-ping via intelligible speech reconstruction using non-acoustic sensor fusion. Pro-ceedings of the 16th ACM/IEEE International Conference on Information Pro-cessing in Sensor Networks, 2017. P. 181-192. – URL: https: //doi.org/10.1145/3055031.3055088 – (data obrashheniya: 25.11.2020).

35. Yan Michalevsky, Dan Boneh, and Gabi Nakibly. Gyrophone: Rec-ognizing Speech from Gyroscope Signals. 23rd USENIX Security Symposium (USENIX Security 14), 2014. P. 1053-1067.

36. Nirupam Roy and Romit Roy Choudhury. Listening through a Vibra-tion Motor. Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services, 2016. P. 57-69. – URL: https://doi.org/10.1145/2906388.2906415 – (data obrashheniya: 30.11.2020).

37. Teng Wei, Shu Wang, Anfu Zhou, and Xinyu Zhang. Acoustic eaves-dropping through wireless vibrometry. Proceedings of the 21st Annual Interna-tional Conference on Mobile Computing and Networking, 2015. P. 130-141.

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность», Институт радиоэлектроники и информационных технологий – РтФ, Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 19. E-mail: sergey_porshnev@mail.ru

БЕЛЯЕВ Дмитрий Олегович, старший преподаватель Учебно-научного центра «Информационная безопасность», Институт радиоэлектроники и информационных технологий – РтФ, Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 19. E-mail: belyaev-urfu@yandex.ru

PORSHNEV Sergey, Dr.Sc., Professor, head of Educational and research center «Information security», Institute of radio electronics and information technologies – RTF, Ural Federal University.B. N. Yeltsin. 620002, Ekaterinburg, Mira street, 19. E-mail: sergey_porshnev@mail.ru

BELYAEV Dmitry, Senior Lecturer of Educational and research center «Information security», Institute of radio electronics and information technologies – RTF, Ural Federal University.B. N. Yeltsin. 620002, Ekaterinburg, Mira street, 19. E-mail: belyaev-urfu@yandex.ru

УДК 004.056 Вестник УрФО № 4(38) / 2020, с. 22–30

Хорев А.А.

DOI: 10.14529/secur200402

ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ РАСПОЗНАВАНИЯ ОПЕРАТОРОМ ТЕКСТОВЫХ СИМВОЛОВ НА ЭКРАНЕ МОНИТОРА, ПОЛУЧЕННЫХ С РАЗЛИЧНЫМ РАЗРЕШЕНИЕМ

В работе приведено описание специального программного обеспечения для проведения экспериментальных исследований и представленырезультаты экспериментальных исследований распознавания оператором изображений текстовых символов (букв и цифр) на экране монитора, полученных с различным разрешением. На основе обработки экспериментальных данных получены аналитические соотношения для расчета вероятности правильного распознавания оператором букв и цифр (шрифт –TimesNewRoman, кегель – 14 пунктов), выводимых на экран монитора, в зависимости от разрешения изображения.

Ключевые слова: *монитор, разрешение изображения, распознавание текстовых символов.*

Horev A. A.

EXPERIMENTAL STUDIES OF OPERATOR RECOGNITION OF TEXT CHARACTERS ON THE MONITOR SCREEN OBTAINED WITH DIFFERENT RESOLUTIONS

The paper describes special software for conducting experimental studies and presents the

results of experimental studies of operator recognition of images of text symbols (letters and numbers) on the monitor screen obtained with different resolutions. Based on the processing of experimental data, analytical relations were obtained for calculating the probability of correct recognition by the operator of letters and numbers (font –Tim Times New Roman, font –14 points) displayed on the monitor screen, depending on the image resolution.

Keywords: *monitor, the resolution of the image, recognizing the text characters.*

I. Введение

Одним из возможных каналов утечки текстовой информации, обрабатываемой средствами вычислительной техники, является просмотр съемка экранов мониторов с использованием оптико – электронных средств разведки [12].

Экспериментально установлено, что вероятность правильного распознавания формы объекта (в том числе букв и цифр) зависит от зашумленности изображения и его разрешения, а также от размеров объектов, количества их видов (типов) и априорной вероятности их появления (предъявления) [4 – 8,12].

При высоких отношениях сигнал/шум, что характерно для типовых условий использования средств оптико–электронной разведки, вероятность распознавания формы объекта в основном зависит от количества элементов разрешения, укладывающихся на критическом размере изображения объекта и сложности его формы [12].

Проведенный анализ доступной отечественной и иностранной литературы показал, что исследования распознавания текстовых изображений на экранах мониторов в основном затрагивают аспекты автоматизированного распознавания текстов и носят теоретический характер.

Поэтому целью данной работы являются экспериментальные исследования распознавания человеком – оператором текстовых изображений, выводимых на экран монитора, в зависимости от разрешения изображений.

II. Постановка задачи исследования

При распознавании объектовзрительная система работает аналогично оптимальному приемнику, который минимизирует среднюю вероятность ошибки, принимая платы за ошибочные решения, равными единице, а за правильные – равными нулю (критерий идеального наблюдателя). При этом вероятность правильного распознавания простого объекта может быть рассчитана по эмпирической формуле [7]

$$P_p \approx \Phi(Q_1 \cdot q - Q_2), \qquad (1)$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} exp\left(-\frac{t^2}{2}\right) dt$ – интегралвероятности;

q – отношение сигнал/шум с учетом фильтрации, осуществляемой зрительной системой;

Q_1 и Q_2 – коэффициенты, зависящие от объема априорной информации об объектах, которой располагает человек – оператор, и его индивидуальных особенностей.

Ворониным Ю.М. и Павловым Н.И. экспериментально установлено, что для алфавита простых фигур Q_1= 0,62 и Q_2=1,25 (при алфавите размером N = 10) и Q_1= 0,60 и Q_2= 0,85 (при алфавите размером N = 5) [4].

В работе [11] приведены результаты экспериментальных исследованийраспознавания оператором на экране мониторатекстовых символов (букв русского языка и цифр), выводимых на экран монитора, при различных отношениях сигнал/шум (q), измеренных в дБ. Значения коэффициентов Q_1 и Q_2, полученные на основе обработки данных экспериментальных исследований, приведены в табл. 1.

Таблица 1

Рассчитанные значения коэффициентов Q_1 и Q_2

Вид символа	Значение коэффициента Q_1	Значение коэффициента Q_2
Буквы прописные	0,67	5,85
Буквы строчные	0,67	6,97
Цифры	0,74	6,43

Анализ значений коэффициентов Q_1 и Q_2, полученных в [4] и [11], показывает, что веро-

ятность правильного распознавания объекта и текстового символа (прописной буквы) достигает значения $P = 0{,}5$ при отношении сигнал/шум $q \approx 2{,}02$ в [4], и при отношении сигнал/шум $q \approx 2{,}73$ в [11]. Различия в пороговых отношениях сигнал/шум, очевидно, определяются существенными различиями в размерах алфавитов объектов распознавания.

Экспериментально установлено, что высоких отношениях сигнал/шум, вероятность распознаванияобъекта(в том числе, текстового символа) зависит от количества элементов разрешения, укладывающихся на критическом размере изображения объекта и объема априорной информации о распознаваемых объектах, и может быть рассчитана по формуле [7]

$$P_p \approx \Phi(Q \cdot N/N_ф - Q) = \Phi[Q(N/N_ф - 1)], \quad (2)$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} exp(-t^2/2)\, dt$ – интегралвероятности;

N – количество элементов разрешения, укладывающихся на критическом размере изображения объекта;

$N_ф$ – коэффициент распознавания формы объекта (количество элементов разрешения, укладывающихся на критическом размере изображения объекта, при котором вероятность его распознавания равна 0,5);

Q – коэффициент, зависящий от индивидуальных особенностей оператора (дешифровщика) и объема априорной информации о распознаваемых объектах.

Обычно за критический размер объекта принимают его минимальный размер на изображении.

Применим данный подход краспознаваниюоператором символов (букв русского языка и цифр), выводимых на экран монитора.

Размер выводимого на экран символа зависит от нескольких параметров. Одним из них является кегль (размер шрифта). Кегль – размер букв по вертикали, включая нижние и верхние выносные элементы (рис.1).

Рис.1. Кегль шрифта

Кегль измеряется в типографских пунктах. Типографический пункт – единица измерения шрифта. В программах компьютерной верстки широко используется введённый компанией Adobe пункт, равный 1/72 дюйма. Таким образом, в типографии текст с кеглем в 12 пунктов будет иметь высоту 12/72 = 1/6 дюйма.

Изображение на экране формируется из пикселей, размер которых определяется размерами экрана и его разрешением. В таком случае высота символов будет измеряться уже в логических дюймах, которые в дальнейшем переводятся в пиксели.

Число пикселей, приходящихся на один логический дюйм, определяется величиной DPI (dotsperinch) [1, 2]. В семействе операционных систем Windows используется соотношение: 96 пикселей на логический дюйм. Например, текст с кеглем 12 в ОС Windows будет иметь высоту в 1/6 логического дюйма или 16 пикселей.

Число пикселей, приходящихся на логический дюйм экрана, может быть увеличено за счет изменения параметра масштабирования в настройках операционной системы.

Помимо кегля, на размер текста, выводимого на экран, влияют размеры экрана и его разрешение. Высоту символа изображения на экране можно рассчитать по формуле

$$h_m = \frac{h_p \cdot h_{mэ}}{h_{pэ}}, \quad (3)$$

где h_m – высота символа, см;

h_p – высота символа, пикселей;

$h_{mэ}$ – высота экрана, см.;

$h_{pэ}$ – вертикальное разрешение экрана, пикселей.

Разные символы текста имеют различную ширину и высоту. Размеры символов в пикселях приведены в [3].

Таким образом, зная размеры и разрешение экрана, тип шрифта, кегль, коэффициент масштабирования, можно определить размер выводимых на экран символов.

Количество элементов разрешения, укладывающихся на размере изображения символа (N), зависит от разрешающей способности оптико-электронного средства наблюдения, дальности наблюдения и размеров символа на экране монитора [12]

$$N = \frac{10^{-2} \cdot h_m}{\gamma_{оэс} \cdot D_н}, \quad (4)$$

где h_m – размер изображения символа на экране монитора, см;

$\gamma_{оэс}$ – угловое разрешение оптико-электронного средства наблюдения, рад;

$D_н$ – дальность наблюдения (съемки), м.

В дальнейшем параметр изображения N будем называть размером изображения символа, измеренного в элементах разрешения

изображения. Чем больше *N*, тем выше разрешение изображения.

Следовательно, для экспериментальной оценки вероятности распознавания оператором текстовых изображений, выводимых на экран, полученных с различным разрешением, необходимо:

– разработать программный комплекс, позволяющий имитировать вывод текстовых изображений на экран монитора при различных разрешениях изображения;

– провести экспериментальные исследования по оценке вероятности распознавания текстовых изображений, выводимых на экран монитора, при различных разрешениях изображения;

– на основе обработки экспериментальных данных получить аналитические выражения для расчета вероятности распознавания оператором текстовых изображений, выводимых на экран монитора, в зависимости от разрешения изображения.

III. Методика проведения исследований

Для проведения экспериментальных исследований был разработан программный комплекс моделирования текстовых изображений с различным разрешением [10].

Комплекс позволяет генерировать текстовые символы (буквы и цифры) и производить их преобразование таким образом, чтобы на высоте символа умещалось указанное количество элементов разрешения (*N*).

При этом для каждого элемента разрешения значение яркости рассчитывается относительно попавших в него пикселей с использованием линейной интерполяции [10].

Пусть *I* – исходное изображение с разрешением $R \times C$. Необходимо преобразовать его в изображение *J* с разрешением $R' \times C'$. Введем коэффициенты $s_R = R/R'$, $s_C = C/C$.

Теперь для каждого $r' = 1, \ldots, R'$ и $c' = 1, \ldots, C'$ введем обозначения $r_f = r' \cdot s_R$, $c_f = c' \cdot SC$, $r = |r_f|$, $c = |c_f|$, $\Delta r = r_f - r$, $\Delta c = c_f - c$ (рис. 2).

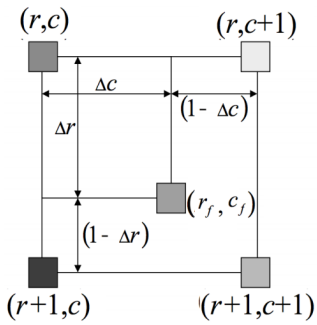


Рис.2. Получение значения яркости пикселя с помощью линейной интерполяции

Значение яркости каждой компоненты пикселя с координатой (r', c') получим по формуле

$$J(r', c') = I(r, c) \cdot (1 - \Delta r) \cdot (1 - - \Delta c) + I(r + 1, c) \cdot \Delta r \cdot (1 - \Delta c) + + I(r, c + 1) \cdot (1 - \Delta r) \cdot \Delta c + I(r + + 1, c + 1) \cdot \Delta r \cdot \Delta c, \quad (5)$$

где $J(r', c')$ – яркость каждой цветовой компоненты пикселя с координатами (r', c') на полученном изображении;

$I(r + 1, c)$ – яркость каждой цветовой компоненты пикселя с координатами *(r, c)* на исходном изображении.

Примеры символов с разным разрешением приведены на рис. 3.

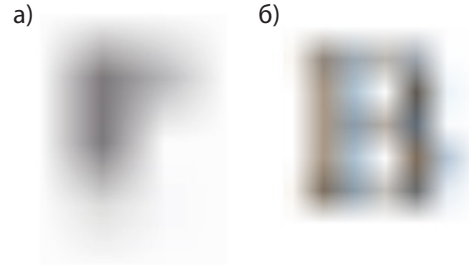


Рис. 3. Изображение буквы «Г», полученное при $N = 3$ (а) и изображение буквы «В», полученное при $N = 8$ (б)

Для написания программного комплекса был выбран язык программирования C++.

Интерфейс программы представлен на рис. 4 [10].

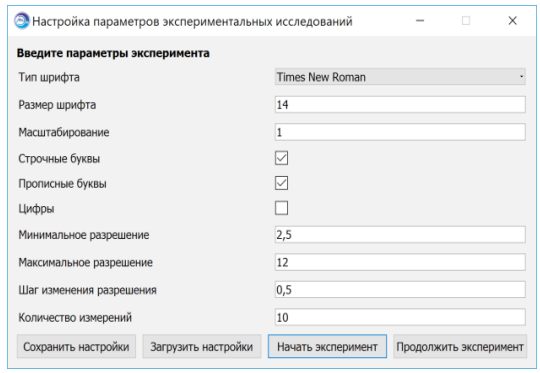


Рис. 4. Интерфейс программы, осуществляющей моделирование текстовых изображений, полученных с разным разрешением

Программный комплекс обеспечивает ввод следующих параметров символов и условий проведения эксперимента: тип шрифта; размер шрифта; коэффициент масштабирования; минимальное и максимальное разрешение; шаг изменения разрешения; пере-

чень символов, выводимых испытуемому (заглавные буквы, строчные буквы, цифры); число экспериментов для каждого символа.

Комплекс позволяет сохранить в отдельный файл параметры настройки условий эксперимента.

В процессе проведения эксперимента на экран монитора случайным образом выводились отдельные символы с выбранным шрифтом, которые оператор должен распознать. При распознавании символа оператор вводил его в соответствующее окно с помощью клавиатуры. Если символ не распознается, оператор нажимал клавишу «пробел» (рис. 5).

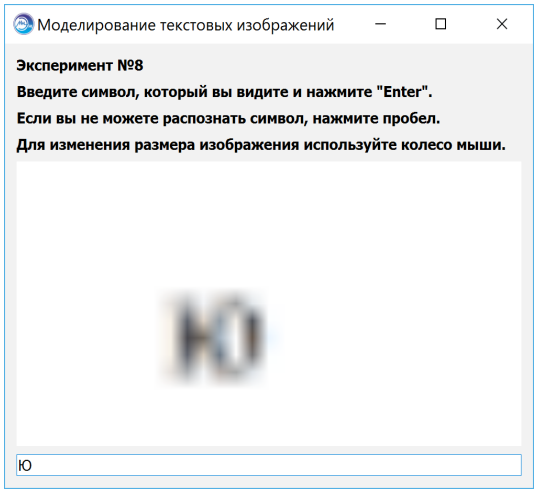


Рис. 5. Интерфейс программы при проведении эксперимента

При необходимости оператор мог менять размер изображения (увеличивать или уменьшать масштаб изображения).

Результаты ответов оператора сохранялись в файл для последующей обработки.

При обработке экспериментальных данных программа рассчитывала вероятность распознавания каждого символа при различных значениях N.

Учитывая, что события распознавания разных символов являются несовместными, для расчета вероятности правильного распознавания групп символов (букв или цифр), предъявляемых в эксперименте, использовалась формула полной вероятности [12]

$$P_p = \sum_{i=1}^{k} P_i^* \cdot P_{pi}, \qquad (6)$$

где P_p – вероятность правильного распознавания группы символов;

P_i^* – априорная вероятность появления i-го символа;

P_{pi} – вероятность правильного распознавания i-го символа при его предъявлении (условная вероятность);

k – число предъявляемых символов.

Априорная вероятность появления букв рассчитывалась на основании частоты встречаемости букв в русском языке

$$P_{i(б)}^* = 0{,}01 \cdot F_i, \qquad (7)$$

где F_i – частота встречаемости i-й буквы в русском языке (табл.2 [9]), %.

Таблица 2

Частота встречаемости букв русского языка

Буква	Частота встречаемости (Fi), %
а	8,01
б	1,59
в	4,54
г	1,7
д	2,98
е	8,45
ё	0,04
ж	0,94
з	1,65
и	7,35
й	1,21
к	3,49
л	4,4
м	3,21
н	6,7
о	10,97
п	2,81
р	4,73
с	5,47
т	6,26
у	2,62
ф	0,26
х	0,97
ц	0,48
ч	1,44
ш	0,73
щ	0,36
ъ	0,04
ы	1,9
ь	1,74
э	0,32
ю	0,64
я	2,01

За априорную вероятность появления цифры принято значение 0,1 (встречаемость цифр принята равновероятной).

Вероятность правильного распознавания i-го символа P_{pi} для каждого значения параметра N рассчитывалась по формуле

$$P_{pi} = \frac{\sum_{m=1}^{M} W_{im}}{V \cdot M} \quad (8)$$

где W_{im} – количество правильных распознаваний *i*-го символа *m* – м оператором;

M – количество операторов, участвующих в эксперименте;

V – количество показов каждого символа.

Экспериментальные исследования проводились в следующей последовательности:

1. Устанавливались параметры символов и условия проведения эксперимента, которые записывались в соответствующий файл.

2. Оператор вводил свое имя, загружал файл с настройками и приступал к проведению эксперимента путем нажатия клавиши «Начать эксперимент».

3. В процессе эксперимента программа на основе введенных параметров генерировала отдельные случайные символы и выводила их на экран монитора. Вначале выводились символы с максимальным значением N из заданного диапазона, затем с установленным шагом разрешение ухудшалось. Таким образом, испытуемые имели возможность наблюдать трансформации, происходящие при уменьшении разрешения, и правильно распознавать символы даже при малых значениях *N*.

4. При вводе каждого символа оператор должен был распознать его. В процессе распознавания оператор с целью создания оптимальных условий наблюдения мог изменять масштаб изображения и расстояние наблюдения. При распознавании символа оператор вводил его в соответствующее окно с помощью клавиатуры. Если символ не распознавался, оператор нажимал клавишу «пробел». После того, как оператор ввел свой ответ, программа генерировала новый символ.

5. После каждого ответа оператора его результаты в автоматическом режиме заносились в соответствующий файл, состоял из записей, содержащих отображаемый символ, его разрешение, смещение относительно элементов разрешения и ответ, данный оператором.

6. Далее проводилась обработка данных эксперимента, которая включала расчет вероятности распознавания каждого символа для каждого значении разрешения и расчет вероятности распознания групп символов с учетом их частоты встречаемости в русском языке.

7. По результатам расчетов строились графики зависимостей вероятностей распознавания символов от разрешения изображения.

8. На основе полученных данных с помощью метода наименьших квадратов определялись значения коэффициентов и для различных символов.

Подбор значений коэффициентов и осуществлялся путем перебора их возможных значений и расчета коэффициента :

$$R^2 = \sum_N \left[P_{\text{р}}(N) - P_p\left(N, Q, N_{\text{ф}}\right)\right]^2 \quad (9)$$

где $P_p(N)$ –вероятность распознавания группы символов, рассчитанная по формуле () по результатам эксперимента для фиксированного значения параметраN;

$P_p\left(N, Q, N_{\text{ф}}\right)$ – вероятность распознавания группы символов, рассчитанная по формуле (2) для фиксированных значений параметров $\left(N, Q, N_{\text{ф}}\right)$.

Программа автоматически рассчитывала значения коэффициентов {$N_ф$ *и Q*}, при которых коэффициент R^2 минимален.

IV. Результаты исследований

В соответствие с методикой, изложенной в п.III, были проведены экспериментальные исследования по распознаванию строчных и прописных букв русского языка, а также цифр в зависимости от разрешения изображений.

В качестве шрифта был выбран шрифт TimesNewRoman с кеглем 14. Масштабирование экрана было установлено в стандартное значение, равное 1.

Разрешение изображения варьировалось в пределах от 2,5 до 11 элементов разрешения, укладывающихся на высоту символов с шагом 0,5. Осуществлялся показ каждого символа с каждым значением разрешения 10 раз с различным значением сдвига относительно элементов разрешения.

Проводить эксперимент со значениями разрешения, выходящими за указанный диапазон, являлось нецелесообразным, так как при больших значениях все символы распознавались с вероятностью 1, а при меньших значениях разрешения вероятность правильного обнаружения становилась равной вероятности случайного выбора правильного варианта.

В экспериментальных исследованиях участвовало 20 операторов. В результате экспериментальных исследований была получена выборка, содержащая 23760 записей о событиях успешного или неуспешного распознавания букв и 7200 событий успешного или неуспешного распознавания цифр.

В процессе обработки эксперименталь-

ных данных были получены зависимости вероятности распознавания прописных и строчных букв русского языка, а также цифр в зависимости от разрешения изображения.

На основе полученных данных с помощью метода наименьших квадратов были определены значения коэффициентов $N_ф$ и Q для различных символов. Их значения приведены в табл. 3.

Полученные значения коэффициентов $N_ф$ попадают в диапазон значений данного коэффициента для уровня распознавания объекта – различие в соответствие с Критериями Джонсона (см. табл. 4 [8]).

На рис. 6–8 приведены графики зависимости вероятности правильного распознавания символов P от значения параметра N, рассчитанные по формуле (2), и полученные экспериментально.

Таблица 3

Результаты расчета коэффициентов Q и $N_ф$

Распознаваемые символы	Параметры	
	Q	$N_ф$
Цифры	3,78	4,50
Строчные буквы	3,37	4,81
Прописные буквы	3,36	4,67
Все символы	3,37	4,74

Таблица 4

Критерии Джонсона

Уровень распознавания	Значение коэффициента $N_ф$
Различие	$N_ф = 4{,}0 \pm 0{,}8$
Опознание	$N_ф = 6{,}4 \pm 1{,}5$

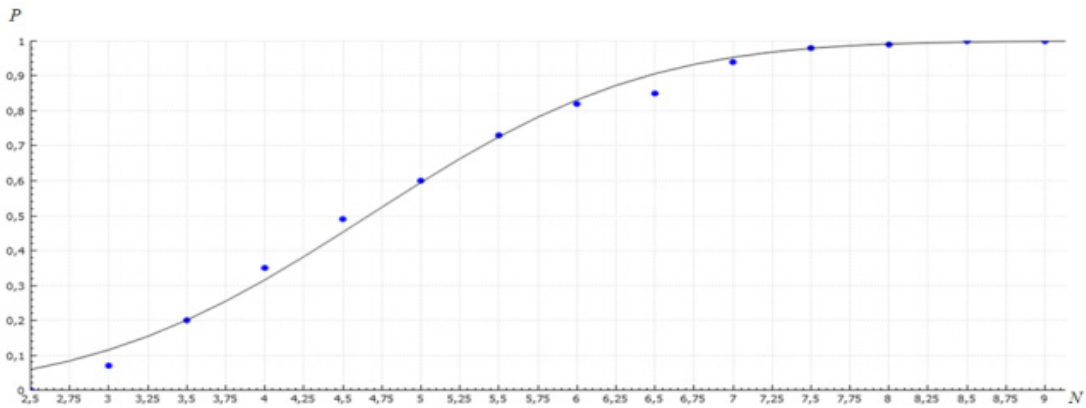


Рис. 6. График зависимости вероятности правильного распознавания прописных букв P от значения параметра N (• –экспериментальные данные)

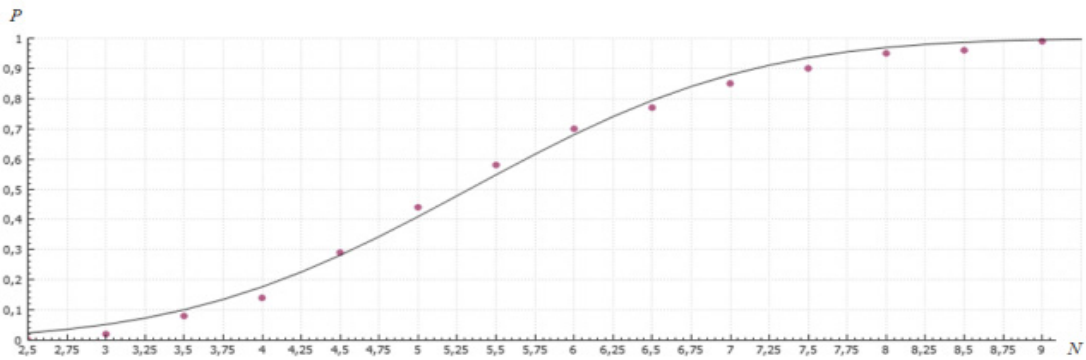


Рис. 7. График зависимости вероятности правильного распознавания строчных букв P от значения параметра N (• – экспериментальные данные)

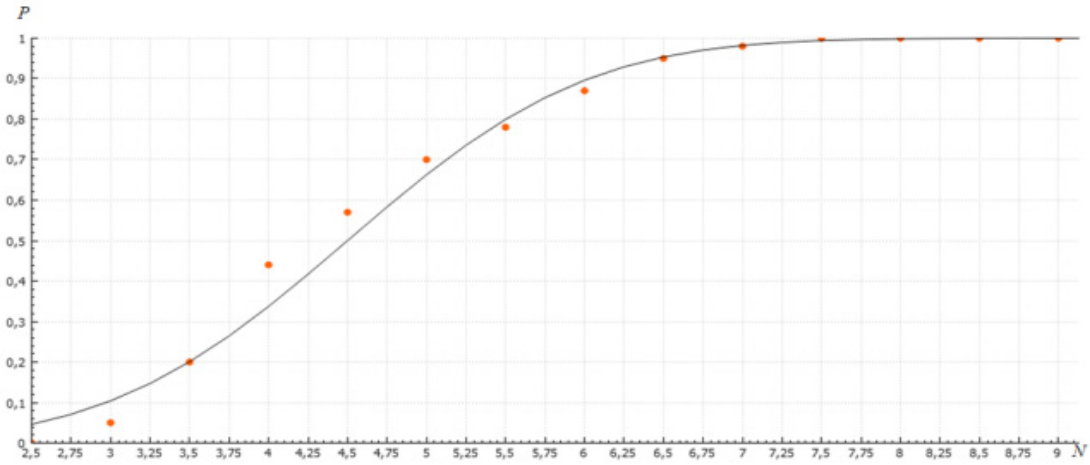


Рис. 8. График зависимости вероятности правильного распознавания цифр *P* от значения параметра *N* (• – экспериментальные данные)

Анализ графиков на рис. 6–8, показывает высокую сходимость результатов расчетов вероятности правильного распознавания текстовых символов по формуле (2) с экспериментальными данными.

V. Заключение

Анализ полученных результатов экспериментальных исследований позволяет сделать следующие выводы:

– зависимость распознавания оператором текстовых символов на изображениях с низким уровнем зашумленности достаточно точно аппроксимируется формулой

$$P_p \approx \Phi[Q(N/N_\phi - 1)],$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} exp(-t^2/2)\, dt$ – интеграл вероятности;

N – количество элементов разрешения, укладывающихся на высоте изображения символа;

N_ϕ – коэффициент распознавания символа (количество элементов разрешения, укладывающихся на высоте изображения символа, при котором вероятность его распознавания равна 0,5);

Q – коэффициент, зависящий вида группы символов (прописные, строчные буквы или цифры) и вида шрифта.

В результате экспериментальных исследований распознавания оператором на экране монитора изображений тестовых символов, написанных шрифтом TimesNewRoman с кеглем 14, полученных с разным разрешением, определены значения коэффициентов N_ϕ и *Q*:

для прописных букв: $N_\phi = 3{,}36$; $Q = 4{,}57$;
для строчных букв: $N_\phi = 3{,}37$; $Q = 4{,}81$;
для цифр: $N_\phi = 3{,}78$; $Q = 4{,}50$.

Полученные значения коэффициентов N_ϕ попадают в диапазон значений данного коэффициента для Критериев Джонсона (уровень распознавания объекта – различие).

Литература

1. DPIandDevice-IndependentPixels [Электронный ресурс]. – URL: https://msdn.microsoft.com/ru-ru/library/windows/desktop/ff684173(v=vs.85).aspx (дата обращения: 17.01.2021).

2. Resolution, DPIandPPI [Электронный ресурс]. – URL: http://www.monarda.se/extra/ppi-test/ppitest_english.htm (дата обращения: 17.01.2021).

3. TimesNewRoman [Электронный ресурс]. – URL: https://www.fonts-online.ru/font/Times-New-Roman (дата обращения: 17.01.2021).

4. Воронин Ю.М., Павлов Н.И. Вероятность распознавания объектов на экране монитора оптико-электронной системы наблюдения// Оптический журнал. – 1994.– № 7. – С. 7 – 11.

5. Глущенко Л.А., Корзун А.М., Павлов Н.И., Силантьев А.Н., Янчук В.В. Определение вероятности распознавания алфавитно-цифровой информации на экране монитора//Труды конференции «Прикладная оптика-2006». [Электронный ресурс]. – URL: http://bibl.laser.nsc.ru/download/2006/PO_sec1.pdf (дата обращения: 17.01.2021).

6. Гулина Ю.С., Колючкин В.Я., Трофимов Н.Е. Распознавание человеком-оператором символов в

условиях сильного зашумления. [Электронный ресурс]. – URL: http://engjournal.ru/articles/492/492.pdf(дата обращения: 17.01.2021).

7. Красильников Н.Н. Теория передачи и восприятия изображений. Теория передачи изображений и ее приложения. – М.: Радио и связь, 1986. – 248 с.

8. Ллойд Дж. Системы тепловидения: Пер. с анг./ Под ред. А.И. Горячева.– М.: Мир, 1978.– 414 с.

9. Ляшевская О.Н., Шаров С. А. Новый частотный словарь русской лексики [Электронный ресурс]. – URL: http://dict.ruslang.ru/freq.php?act=show&dic=freq_letters (дата обращения: 17.01.2021).

10. Моисеев В.Г. Разработка методики расчета вероятности распознавания текстовых изображений, полученных средствами оптико-электронной разведки: магистерская диссертация по направлению 10.04.01 Информационная безопасность. – М.: НИУ МИЭТ, 2017. – 105 с.

11. Хорев А.А. Методика оценки вероятности распознавания текстовых символов на зашумленных изображениях//Вестник УрФО «Безопасность в информационной сфере». – Челябинск, УрФО. – 2019. - № 4(34) – С. 5 – 14.

12. Хорев А.А. Теоретические основы оценки возможностей технических средств разведки: монография. – М.: МО РФ, 2000. – 255 с.

References

1. DPIandDevice-IndependentPixels [Elektronnyy resurs]. – URL: https://msdn.microsoft.com/ru-ru/library/windows/desktop/ff684173(v=vs.85).aspx (data obrashcheniya: 17.01.2021).

2. Resolution, DPIandPPI [Elektronnyy resurs]. – URL: http://www.monarda.se/extra/ppi-test/ppitest_english.htm (data obrashcheniya: 17.01.2021).

3. TimesNewRoman [Elektronnyy resurs]. – URL: https://www.fonts-online.ru/font/Times-New-Roman (data obrashcheniya: 17.01.2021).

4. Voronin YU.M., Pavlov N.I. Veroyatnost' raspoznavaniya ob"yektov na ekrane monitora optiko-elektronnoy sistemy nablyudeniya// Opticheskiy zhurnal. – 1994. – № 7. – S. 7 – 11.

5. Glushchenko L.A., Korzun A.M., Pavlov N.I., Silant'yev A.N., Yanchuk V.V. Opredeleniye veroyatnosti raspoznavaniya alfavitno-tsifrovoy informatsii na ekrane monitora//Trudy konferentsii «Prikladnaya optika-2006». [Elektronnyy resurs]. – URL: http://bibl.laser.nsc.ru/download/2006/PO_sec1.pdf (data obrashcheniya: 17.01.2021).

6. Gulina YU.S., Kolyuchkin V.YA., Trofimov N.Ye. Raspoznavaniye chelovekom-operatorom simvolov v usloviyakh sil'nogo zashumleniya. [Elektronnyy resurs]. – URL: http://engjournal.ru/articles/492/492.pdf (data obrashcheniya: 17.01.2021).

7. Krasil'nikov N.N. Teoriya peredachi i vospriyatiya izobrazheniy. Teoriya peredachi izobrazheniy i yeye prilozheniya. 248 s– M.: Radio i svyaz', 1986.

8. Lloyd Dzh. Sistemy teplovideniya: Per. s ang./ Pod red. A.I. Goryacheva. 414 s.– M.: Mir, 1978.

9. Lyashevskaya O.N., Sharov S. A. Novyy chastotnyy slovar' russkoy leksiki [Elektronnyy resurs]. – URL: http://dict.ruslang.ru/freq.php?act=show&dic=freq_letters (data obrashcheniya: 17.01.2021).

10. Moiseyev V.G. Razrabotka metodiki rascheta veroyatnosti raspoznavaniya tekstovykh izobrazheniy, poluchennykh sredstvami optiko-elektronnoy razvedki: magisterskaya dissertatsiya po napravleniyu 10.04.01 Informatsionnaya bezopasnost'. – M.: NIU MIET, 2017. – 105 s.

11. Khorev A.A. Metodika otsenki veroyatnosti raspoznavaniya tekstovykh simvolov na zashumlennykh izobrazheniyakh//Vestnik UrFO «Bezopasnost' v informatsionnoy sfere». – Chelyabinsk, UrFO. – 2019. - № 4(34) – S. 5 – 14.

12. Khorev A.A. Teoreticheskiye osnovy otsenki vozmozhnostey tekhnicheskikh sredstv razvedki: monografiya. – M.: MO RF, 2000. – 255 s.

ХОРЕВ Анатолий Анатольевич, доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность», «Национальный исследовательский университет «Московский институт электронной техники». 124498, г. Москва, г. Зеленоград, площадь Шокина, дом 1. E-mail: horev@miee.ru

HOREV Anatoly, doctor of technical Sciences, Professor, head of the Department "Information security", National Research University of Electronic Technology. 124498, Moscow, Zelenograd, Shokin square, house 1. E-mail: horev@miee.ru

УДК 004.056.2 + 621.396.674 Вестник УрФО № 4(38) / 2020, с. 31–43

Войтович В.В., Петраш Ю.В., Белоусов М. М., Юнгайтис Е.М., Ершов А.В., Войтович Н.И.

DOI: 10.14529/secur200403

ДИПОЛЬНАЯ АНТЕННА С КРУГОВОЙ ДИАГРАММОЙ НАПРАВЛЕННОСТИ В ПЛОСКОСТИ ВЕКТОРА Е ДЛЯ ПРОВЕРКИ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ СИСТЕМ ПОСАДКИ ВОЗДУШНЫХ СУДОВ

В работе представлены результаты исследований всенаправленной дипольной антенны, предназначенной для установки на беспилотный летательный аппарат категории мини — БПЛА. Антенна формирует круговую диаграмму направленности в горизонтальной плоскости с горизонтальной поляризацией поля излучения. Неравномерность диаграммы направленности исследуемой антенны в свободном пространстве в горизонтальной плоскости составляет ±0,2 дБ. Антенна содержит минимальное количество элементов фидерного тракта, имеет удобную для практической реализации конструкцию.

Ключевые слова: *целостность навигационной информации, ГРМ, дипольная антенна, беспилотный летательный аппарат, мини-БПЛА.*

Voitovich V.V., Petrash Yu.V., Belousov M.M., Yungaitis E.M., Ershov A.V., Voitovich N.I.

DIPOLE ANTENNA WITH CIRCULAR RADIATION PATTERN IN THE E-PLANE FOR VALIDATION THE INTEGRITY OF THE AIRCRAFT LANDING SYSTEMS INFORMATION

The paper presents the results of studies of an omnidirectional dipole antenna designed for installation on an unmanned aerial vehicle of the mini-UAV category. The antenna forms a circular radiation pattern in the horizontal plane with horizontal polarization of the radiated field. Irregularity of the radiation pattern of the antenna under study in free space in the horizontal plane is ± 0.2 dB. The antenna contains a minimum number of elements of the feeder path. It has convenient for practical implementation design.

Keywords: *the integrity of radio navigation information, GRM, omnidirectional dipole antenna, unmanned aerial vehicle, mini UAV.*

Введение

Одним из основных факторов обеспечения безопасности полетов воздушных судов на критических этапах захода на посадку и посадки является (наряду с непрерывностью обслуживания) целостность информации, создаваемой в пространстве курсовым и глиссадным радиомаяками (КРМ и ГРМ) инструментальной системы посадки (ILS) [1]. По определению Международной Организации Гражданской Авиации (ИКАО) целостность – это качество ILS, соответствующее степени уверенности в том, что обеспечиваемая данным средством информация является правильной.

Целостность необходима для обеспечения того, чтобы воздушное судно, осуществляющее заход на посадку, имело малую вероятность неправильного наведения.

Подсчет целостности (***I***) ILS выполняется путем определения вероятности (***P***) передачи необнаруженного излучения неправильного сигнала: ***I = 1 – P***.

Признается, что среднее количество P_c авиационных происшествий со смертельным исходом во время посадки по причине выхода из строя систем в целом или недостатков в ней, куда входит наземное оборудование, воздушное судно и пилот, не должно превышать показатель $P_c = 1 \times 10^{-7}$ [1]. Этот критерий часто называют общим показателем риска. Целостность включает способность системы обеспечить пользователя своевременными и обоснованными предупреждениями.

Нарушение целостности информации может произойти, если выход сигнала за пределы допустимого отклонения либо не опознается контрольным оборудованием, либо цепи контрольного оборудования не могут исключить излучение неправильного сигнала; подобное нарушение, если оно вызывает большую погрешность, может привести к опасной ситуации.

Контрольные устройства, выполняющие постоянный мониторинг излучаемого сигнала в эфире, устанавливаются в точках в ближней зоне действия радиомаяков. Поэтому необходимы тщательные летные и наземные обследования в периодические интервалы времени для обеспечения гарантии целостности информационного сигнала в эфире во всей зоне действия.

Курсовой и глиссадный радиомаяки для подтверждения выходных характеристик при вводе в эксплуатацию, периодически в процессе их эксплуатации и в некоторых специальных случаях подвергаются лётным проверкам. Для целей лётных проверок наземных средств радиотехнического обеспечения полетов используется специальный самолёт-лаборатория, на котором установлены измерительные приёмники [2].

Однако, известен другой способ лётной проверки наземных средств радиотехнического обеспечения полётов, решающий задачу повышения оперативности проверок радиомаяков, снижающий затраты на выполнение проверок. Упомянутый другой способ заключается в том, что в качестве воздушного судна для лётной проверки применяют дистанционно пилотируемый летательный аппарат (ДПЛА) [3].

Для приёма сигналов курсового и глиссадного радиомаяков на борту ДПЛА категории Мини [4], например, квадрокоптера, требуется легкая антенна с круговой диаграммой направленности в горизонтальной плоскости с горизонтальной поляризацией поля излучения (в плоскости вектора E). Настоящая статья посвящена исследованиям, направленным на создание требуемой антенны.

Как известно, подобная антенна требуется при решении и других технических задач. Существует несколько способов получить круговую диаграмму направленности антенны в горизонтальной плоскости. Примером может служить турникетная антенна, состоящая из двух взаимно перпендикулярных полуволновых или петлевых диполей с токами в диполях сдвинутыми между собой на 90 градусов. Первая турникетная антенна была изобретена G. H. Brownв 1935 году [5].

В работах [6-16] представлены способы обеспечения круговой диаграммы направленности за счет использования пространственной антенной решётки излучающих элементов. Однако, такие антенны громоздки, имеют большой вес.

Другой способ — использование рамочных антенн, обладающих малыми габаритами в сравнении с длиной волны на центральной частоте. При этом рамочные антенны имеют существенный недостаток — узкую полосу согласования с фидером [17].

Существенно более простой конструкцией обладает угловой диполь, изобретенный P.S. Carter в 1938 г. [18]. Отличие ДН от окружности составляет $\pm$ 3 дБ.

В настоящей работе представлены результаты исследований дипольной антенны с горизонтальной поляризацией поля излучения с круговой диаграммой направленности в горизонтальной плоскости, предназначенной для установки на беспилотный летательный аппарат категории Мини-БПЛА.

Постановка задачи

Поставим своей задачей создать антенну на основе диполя Герца. Вибраторная антенна (вибратор или говорят диполь Герца) известна со времени открытия в 1888 г. Генрихом Герцем электромагнитных волн и экспериментального подтверждения теории Джеймса Максвелла [19, 20]. Вибратор Герца представлял собой совершенно прямую медную проволоку, длиной 2,0 м и толщиной 5 мм. В середине проволока была разрезана с образованием двух плеч и зазора между ними для введения в зазор возбуждающего искрового промежутка. Два маленьких металлических шарика были насажены непосредственно на проволоку на концах, примыкающих к зазору, и соединены с полюсами индукционной катушки. Между шариками происходил электрический разряд. На противоположных концах проволоки были расположены два шара диаметром 30 см, изготовленные из толстого цинкового листа.

Диаграмма направленности (ДН) диполя Герца в свободном пространстве имеет вид тороида, ось которого направлена вдоль оси диполя. ДН диполя Герца, расположенного в горизонтальной плоскости, имеет в горизонтальной плоскости (в плоскости вектора E) вид восьмёрки с нулевыми уровнями, направленными вдоль оси диполя.

В связи с применением в телевизионном вещании волн горизонтальной поляризации появилась потребность в антенне с горизонтальной поляризацией со всенаправленной ДН в горизонтальной плоскости с целью приёма телевизионных сигналов от нескольких разнесённых в пространстве телевизионных станций. При этом под всенаправленной диаграммой направленности в горизонтальной плоскости подразумевается ДН, в которой уровни минимумов в известной мере высоки. Для обеспечения всенаправленного приёма P.S. Carter в 1938 г. предложил диполь, плечи которого в горизонтальной плоскости расположены под углом 90° относительно друг друга [18]. ДН полуволнового углового диполя имеет неравномерность $\pm$ 3 дБ. Во многих практических случаях это слишком большая

неравномерность. С целью снижения отличия формы ДН от круга в данной работе предложено выполнить плечи диполя в виде прописной буквы **Г**.

Интуитивно понятно, что изгиб плеч диполя приведёт к "заплыванию" нулевого уровня в ДН в направлении исходной оси диполя. Естественно стремление получить при этом ДН без нулевых уровней в других направлениях. В той плоскости, в которой выполнен изгиб плеч диполя, необходимо получить ДН, близкую по форме к круговой.

Будем полагать, что общая длина диполя близка к половине длины волны. Диаметр проводников плеч диполя много меньше длины волны. Диполь возбуждается в его центре, в зазоре. При этом для компенсации реактивной составляющей входного сопротивления диполя применён согласующий отрезок фидера. Материал проводников диполя — идеально проводящий. Исследуем влияние геометрии плеч диполя и величины зазора между плечами на формирование диаграммы направленности антенны.

Физическая модель

Исследуемая симметричная вибраторная антенна представляет собой полуволновый диполь, плечи которого имеют изгиб в некоторой плоскости. Антенна возбуждается в зазоре между плечами диполя источником, включенным последовательно с согласующим устройством в виде отрезка коаксиальной линии передачи. С плечами вибратора соединён также отрезок короткозамкнутой двухпроводной линии. Длина двухпроводной линии равна четверти длины волны на средней рабочей частоте. Короткозамкнутый четвертьволновый отрезок двухпроводной линии выполняет роль симметрирующего устройства. Предполагается, что диполь и симметрирующее устройство выполнены из цилиндрических проводников, радиусы цилиндров которых много меньше длины волны. Все проводники выполнены из идеально проводящего материала. Антенна расположена в свободном пространстве. Возбуждающая мощность к антенне подводится с помощью коаксиального кабеля.

Конструкция антенны

В макете дипольной антенны с зазором (рис.1) каждое плечо диполя состоит из двух частей: основной (исходной) части и ортогональной части.

Части плеча расположены по отношению

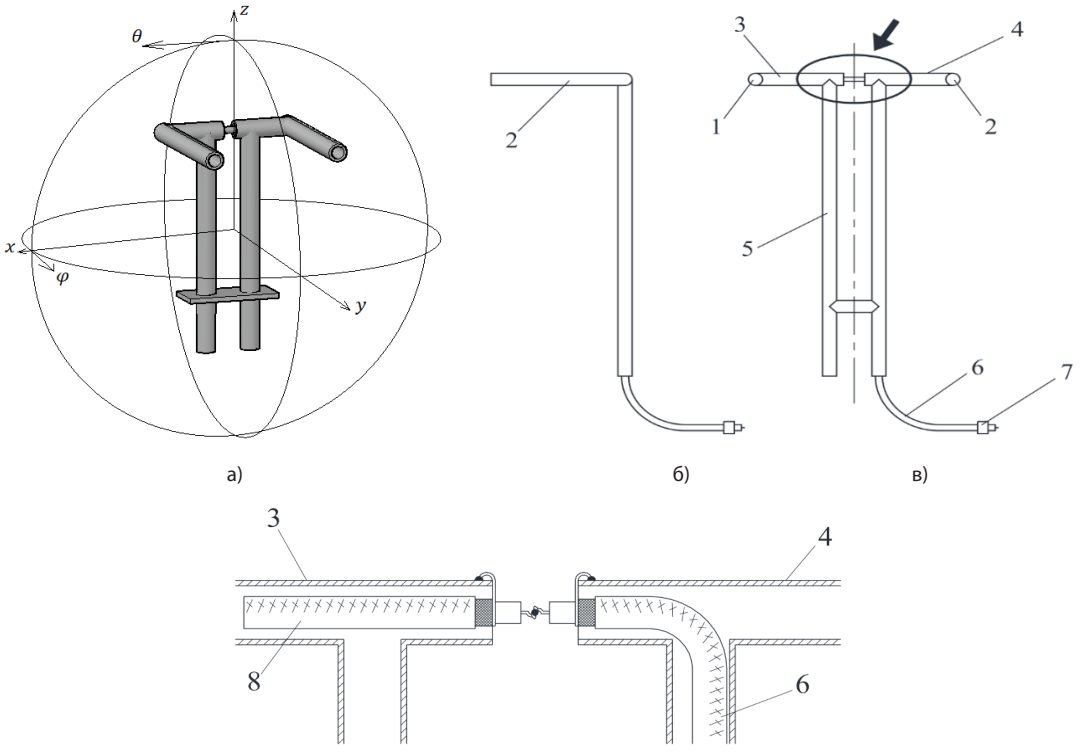


Рис. 1. Конструкция антенны; а) вид в изометрии и система координат,
б) вид сбоку, в) фронтальный вид, г) вид по стрелке;
1, 2 — ортогональная часть диполя, 3, 4 — исходная часть диполя, 5 — плечи симметрирующего устройства,
6 — коаксиальный кабель, 7 — соединитель радиочастотный, 8 — согласующий отрезок кабеля.

друг к другу под углом равным 90°. По форме одно плечо имеет вид прописной буквы Г, а второе имеет вид её зеркального отражения. Буква Г и её зеркальное отражение направлены к центру (к зазору) диполя своей верхней (горизонтальной) частью. Буква Г и её зеркальное отражение лежат в одной и той же плоскости и совместно формируют П-образный диполь с зазором. Для исключения антенного эффекта фидера в антенне использовано симметрирующее устройство, представляющее собой четвертьволновый отрезок двухпроводной линии передачи с режимом короткого замыкания на конце. Плечи симметрирующего устройства перпендикулярны к плоскости, в которой лежит диполь. Плечи диполя и плечи симметрирующего устройства выполнены из полой трубки с внешним диаметром 8 мм. В качестве фидера антенны применён коаксиальный кабель РК-50-2-11 с соединителем радиочастотном на одном конце. Коаксиальный кабель проложен внутри трубки одного из плеч симметрирующего устройства, далее проложен внутри одного из плеч диполя в сторону зазора между плечами. На выходе из плеча, в зазоре, внешний проводник коаксиального кабеля имеет гальванический контакт с плечом. Центральный проводник проложен через зазор между плечами и соединён с центральным проводником согласующего отрезка кабеля, расположенном во втором плече. Внешний проводник согласующего отрезка кабеля имеет в зазоре гальванический контакт со вторым плечом диполя. Второй, холостой, конец согласующего отрезка кабеля ни с чем не соединён.

Согласующий отрезок коаксиальной линии с режимом холостого хода на конце применён для компенсации индуктивной части входного сопротивления антенны. При этом емкостная составляющая указанного согласующего отрезка может быть рассчитана по формулам:

$$\dot{Z} = -jZ_0 \mathrm{ctg}\left(\frac{2\pi\sqrt{\varepsilon_r}}{\lambda} l\right), \quad (1)$$

$$C = -\frac{1}{j\omega\dot{Z}}, \quad (2)$$

где: $\dot{Z}$ — входное сопротивление согласующего отрезка коаксиальной линии с режимом холостого хода на конце;

Z_0 — волновое сопротивление согласующего отрезка коаксиальной линии;

λ — длина волны;

ε_r — относительная диэлектрическая проницаемость диэлектрика согласующего отрезка;

l — длина согласующего отрезка коаксиальной линии передачи с режимом холостого хода на конце;

C — емкостная составляющая согласующего отрезка коаксиальной линии передачи с режимом холостого хода на конце;

ω — круговая частота.

Методы исследования

Воспользуемся двумя теоретическими методами решения поставленной задачи. Во-первых, воспользуемся методом решения интегрального уравнения относительно тока в проводниках диполя в тонкопроволочном приближении [21,22].

Во-вторых, в последующих работах используем широко известное решение краевой задачи в строгой дифракционной постановке прямыми численными методами. В строгой дифракционной постановке краевая электродинамическая задача, сформулированная для непрерывного континуума, редуцируется к проекционно-сеточной модели. Сеточная модель строится с надлежащим выбором базисных и пробных функций, удовлетворяющих граничным условиям, условиям полноты и ортогональности, условиям излучения и условиям Мейкснера. Единственность решения и минимум невязки решения в выбранном конечномерном пространстве базисных функций гарантируется проекционным методом решения дифракционной задачи.

В отношении первого решения заметим следующее. Исследуемая антенна представляет собой конструкцию из совокупности цилиндрических проводников, диаметр которых много меньше длины волны, а продольный размер велик по сравнению с диаметром проводников. Это обстоятельство позволяет при решении задачи использовать тонкопроволочное приближение. Для создания математической модели антенны воспользуемся теоремой взаимности в интегральной форме:

$$\int_{\upsilon} \vec{j}_1 \vec{E}_2 d\upsilon = \int_{\upsilon} \vec{j}_2 \vec{E}_1 d\upsilon \quad (3)$$

где $\vec{E}_1$, $\vec{E}_2$ — напряжённости электрических полей, удовлетворяющих принципу излучения на бесконечности и создаваемые независящими друг от друга сторонними токами проводимости $\vec{j}_1$, $\vec{j}_2$, соответственно;

υ — некоторый произвольный объём, в котором расположены источники $\vec{j}_1$, $\vec{j}_2$.

Исследуемая антенна представлена совокупностью *N* диполей, называемых «истинными источниками», с неизвестными комплексными амплитудами тока, для определения которых вводится в рассмотрение *N* «пробных» диполей. Рассмотрено взаимодействие двух линейных электрических источников, «истинного» и «пробного», расположенных в ближней зоне. Связь между пробным и истинным источниками определена с помощью взаимного сопротивления. Полученные результаты обобщаются на систему *N* электрически коротких «истинных» диполей, имеющих синусоидальное распределение тока, электромагнитно связанных с *N* «пробными» диполями. Каждый из диполей анализируемой антенны образован из двух соседних сегментов, на которые разбиты проводники антенны. При этом плечи соседних диполей перекрываются, что позволяет аппроксимировать распределённый вдоль антенны ток с достаточно хорошим приближением.

Далее составлена система линейных алгебраических уравнений (СЛАУ), решаемая относительно амплитуд токов в данных диполях, являющихся коэффициентами кусочно-синусоидальной аппроксимации функции распределения тока вдоль проводников анализируемой антенны. На основе найденного распределения тока определяются входной импеданс и ДН антенны.

Описанная выше методика аналогична известному методу Ричмонда анализа проволочных антенн. Методика включает три основных этапа:

1) разбиение проводников антенны на электрически короткие сегменты, из которых составляются диполи; задание возбуждения в виде вектора [V], элементы которого соответствуют значениям напряжений источников диполей;

2) составление матрицы [Z] взаимных сопротивлений «истинных» и «пробных» диполей, элементы которой для *m*-го «пробного» и *n*-го «истинного» диполей вычисляются по формуле:

$$Z_{mn} = -\int_{l_{n-1}}^{l_n} \frac{\sin k(l_n - l)}{\sin k d_{n-1}} \vec{h}_{n-1} \vec{E}_m dl - \int_{l_n}^{l_{n+1}} \frac{\sin k(l - l_n)}{\sin k d_n} \vec{h}_n \vec{E}_m dl, \quad (4)$$

где l — координата вдоль оси сегмента;

l_n — продольная координата стыка *n*-1-го и *n*-го сегментов;

k — волновое число;

d_{n-1} и d_n — длины сегментов с номерами n-1 и n соответственно;

$\vec{h}_{n-1}$ и $\vec{h}_n$ — касательные орты соответствующих сегментов, направлены в сторону положительного направления тока;

$\vec{E}_m$ — напряженность электрического поля в точке интегрирования, создаваемая *m*-ным «пробным» диполем;

3) решение СЛАУ относительно комплексных амплитуд функции, аппроксимирующей токовую функцию, в виде вектора [I]:

$$[V]=[Z][I] \quad (5)$$

Для реализации данного метода найдены соотношения для вычисления напряжённости электрического поля диполя с синусоидальным распределением тока, первое плечо которого имеет длину d_1, второе — d_2, а угол между плечами отличается от 180° на величину α (рис. 2). Поле определяется в точке наблюдения $M(\rho, 0, z_m)$. Решение найдено на основе уравнений Максвелла с помощью метода запаздывающего векторного электрического потенциала.

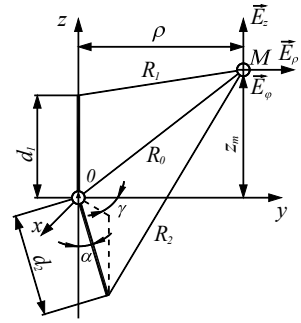


Рис. 2. Расположение диполя в цилиндрической системе координат

Электрическое поле $\vec{E}_m = \vec{E}(E_z, E_\rho, E_\varphi)$ такого диполя в цилиндрической системе координат определяется соотношениями:

$$E_z = E_{||}^{(1)} + E_{||}^{(2)} \cos\alpha + E_{\perp}^{(2)} \sin\alpha \quad (6)$$

$$E_\rho = E_\rho^{(1)} + E_{||}^{(2)} \sin\alpha \cos\gamma + E_{\perp}^{(2)} \cos\alpha \cos\gamma \quad (7)$$

$$E_\varphi = -E_{||}^{(2)} \sin\alpha \sin\gamma - E_{\perp}^{(2)} \cos\alpha \sin\gamma, \quad (8)$$

где

$$E_{||}^{(1)} = \frac{-iWI_0}{4\pi \sin kd_1} \left\{ \frac{e^{-ikR_1}}{R_1} - \frac{e^{-ikR_0}}{R_0} \cos kd_1 - \frac{e^{-ikR_0}}{R_0} \frac{\sin kd_1}{k} \left(ik + \frac{1}{R_0} \right) \frac{z_m}{R_0} \right\} \quad (9)$$

$$E_{\perp}^{(1)} = \frac{iWI_0}{4\pi\rho \sin kd_1} \left\{ \frac{\sin kd_1}{k} \frac{e^{-ikR_0}}{R_0} - \frac{z_m^2}{R_0^2} \frac{\sin kd_1}{k} e^{-ikR_0} \left(ik + \frac{1}{R_0} \right) + \right.$$
$$\left. + \frac{z_m - d_1}{R_1} e^{-ikR_1} - \frac{z_m}{R_0} \cos kd_1 e^{-ikR_0} \right\}; \quad (10)$$

$$E_{||}^{(2)} = \frac{-iWI_0}{4\pi \sin kd_2} \left\{ \frac{\sin kd_2}{kR_0^2} e^{-ikR_0} \left(ik + \frac{1}{R_0} \right) z_m - \frac{e^{-ikR_0}}{R_0} \cos kd_2 + \frac{e^{-ikR_2}}{R_2} \right\} \quad (11)$$

$$E_{\perp}^{(2)} = \frac{iWI_0}{4\pi\rho \sin kd_2} \left\{ -\frac{\sin kd_2}{k} \frac{e^{-ikR_0}}{R_0} + \frac{z_m^2}{R_0^2} \frac{\sin kd_2}{k} e^{-ikR_0} \left(ik + \frac{1}{R_0} \right) + \right.$$
$$\left. + \frac{z_m + d_2}{R_2} e^{-ikR_2} - \frac{z_m}{R_0} \cos kd_2 e^{-ikR_0} \right\}; \quad (12)$$

$$R_0 = \sqrt{\rho^2 + z_m{}^2}; \quad (13)$$

$$R_1 = \sqrt{\rho^2 + \left(z_m - d_1\right)^2} \quad (14)$$

$$R_2 = \sqrt{\left(\rho - d_2 \sin\alpha\cos\gamma\right)^2 + \left(z_m + d_2\cos\alpha\right)^2 + \left(d_2 \sin\alpha\sin\gamma\right)^2} \quad (15)$$

γ — угол между проекцией второго плеча диполя на плоскость xOy и осью Oy;

W — волновое сопротивление среды;

I_0 — амплитуда тока в диполе.

Оба решения реализованы в виде программ на ЭВМ и использованы для численных исследований.

Результаты численных исследований

Введём буквенные обозначения элементов антенны. Обозначим буквой А исходную (до изгиба) часть плеча, буквой В — загнутую часть плеча диполя. Буквой L_1 обозначим длину симметрирующего устройства, D — расстояние между трубками СУ, R_1 — радиус трубок плеч диполя, R_2 — радиус труб симметрирующего устройства, L_2 — длина согласующего отрезка кабеля. На рис. 3, в качестве примера, представлено распределение тока вдоль плеч диполя, плеч и короткозамыкателя симметрирующего устройства, на проводниках, продолжающих плечи СУ. Распределение тока на участке В от кончика плеча до изгиба на каждом плече диполя имеет характер стоячей волны. На участке А от изгиба до точки подключения к плечу диполя плеча СУ распределение тока соответствует распределению смешанной волны. Вдоль плеч СУ и на короткозамыкателе распределение тока близко к стоячей волне тока. Отличие от нулевого значение тока на входе СУ объясняется тем фактом, что СУ является отрезком открытой линии передачи, частично излучающей электромагнитные волны в окружающее пространство.

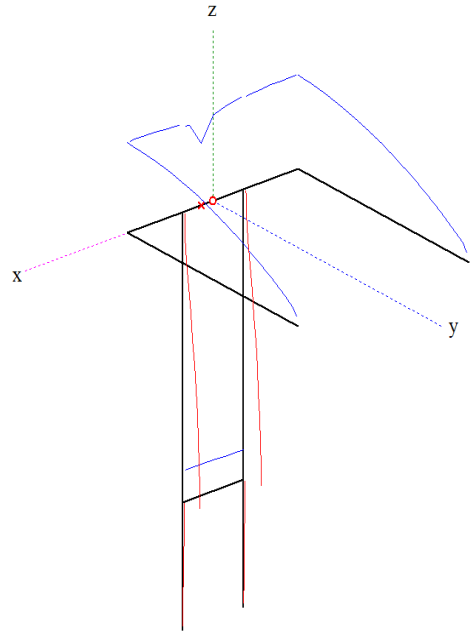


Рис. 3. Распределение тока на излучающих и конструктивных элементах антенны на частоте 954 МГц.

Ток на проводниках, продолжающих плечи СУ, пренебрежимо мал.

Рассмотрено несколько вариантов антенн. Диаграммы направленности (ДН) антенн в декартовой системе координат представлены на рис. 4. Наилучшие характеристики ДН получены при следующих размерах элементов антенны:

A=56 мм, B=68 мм, L1=76 мм, D=20 мм, R1=4 мм, R2=4 мм, L2=14.5 мм.

Общая длина вибратора 192 мм.

№ варианта	1	2	3	4	5	Уголковый вибратор
Длина средней части (А), мм	36	46	56	66	76	—
Длина загнутой части (В), мм	78	73	68	63	58	78
Максимальное отклонение ДН от окружности, %	14	7,4	2,4	8,5	16	42
Максимальное отклонение ДН от окружности, дБ	1,1	0,62	0,2	0,71	1,3	3,1

Экспериментальные результаты

Антенна для установки на квадракоптер для измерения характеристик ПРМГ в сумме с кабелем и соединителем радиочастотным весит 87,2 грамма. В том числе: антенна 35,2 грамм, кабель РК-50-2-12 длиной 75 см 12 грамм, соединитель радиочастотный СР-50-135ПВ 40 гр. Экспериментальное исследование основных электродинамических параметров всенаправленной дипольной антенны выполнено в лаборатории каф. КиПР ЮУрГУ. В качестве измерительного оборудования использовался векторный анализатор цепей ОБЗОР-103. В качестве передающей антенны использована рупорная антенна глиссадного радиомаяка.

На рис 6. Представлено фото антенны с диэлектрическим обтекателем, защищающим область возбуждения антенны от воздействия дождя и снега.

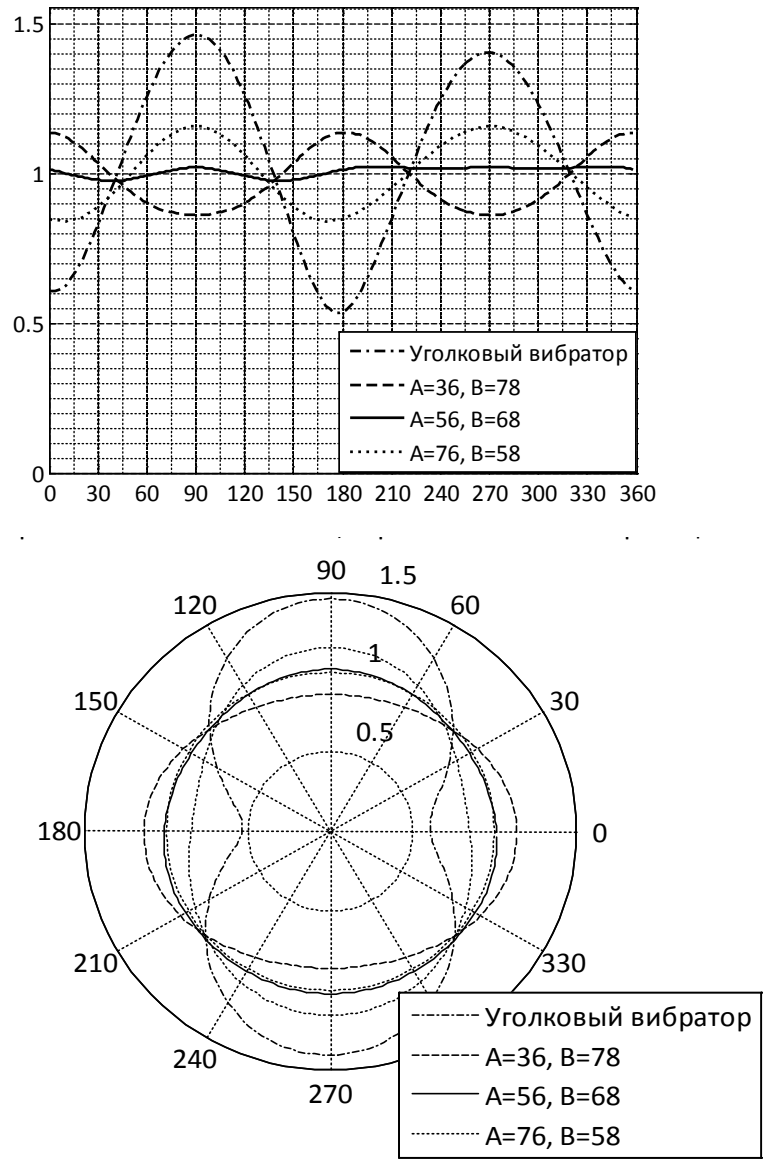
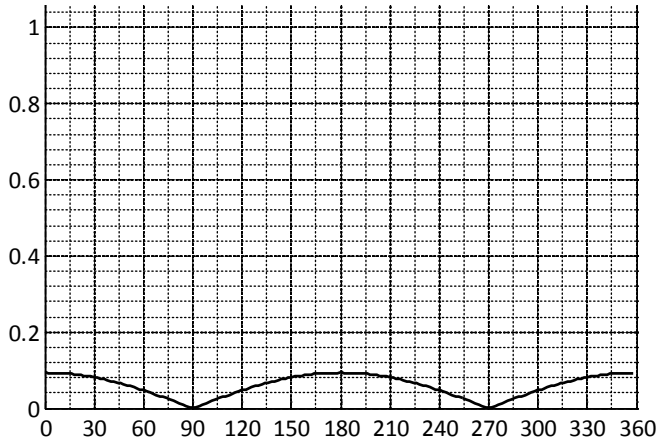
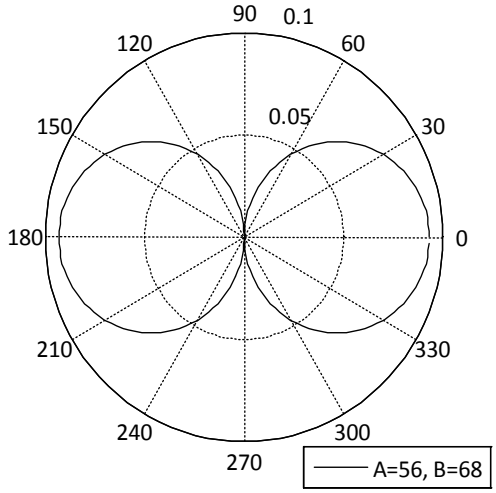


Рис. 4. Диаграммы направленности горизонтальной составляющей поля излучения диполя с плечами Г-образной формы в горизонтальной плоскости.



а)



б)

Рис.5. Диаграмма направленности антенны в горизонтальной плоскости для вертикальной составляющей (кросскомпоненты) напряжённости электрического поля (A=56, B=68 мм); а) в декартовой системе координат, б) в полярной системе координат

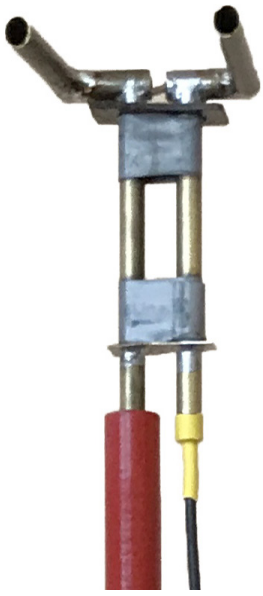


Рис.6. Фото макета антенны

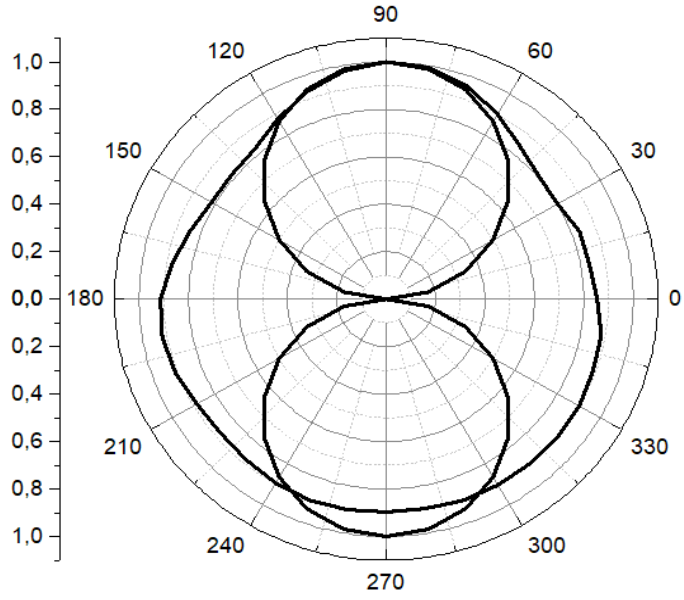


Рис.7. Диаграммы направленности макета антенны и классического диполя на частоте 1000 МГц

На рис.7 представлена диаграмма направленности в Е-плоскости на частоте 1000 МГц макета всенаправленной дипольной антенны и классического диполя (в виде восьмёрки).

Уровень отклонения диаграммы направленности от окружности равен $\pm$ 0,1 (минус 20 дБ).

Обсуждение

Как указывалось выше, диполь Герца, будучи расположенным в горизонтальной плоскости, имеет в горизонтальной плоскости (в плоскости вектора Е) вид восьмёрки, с нулевыми уровнями, направленными вдоль оси диполя. Диполь, предложенный P.S. Carter, плечи которого в горизонтальной плоскости расположены под углом 90° относительно друг друга имеет неравномерность ± 3 дБ. Для ряда применений антенны с горизонтальной поляризаций это слишком большая величина. С целью снижения отличия формы ДН от круга в данной работе предложено выполнить плечи диполя в виде прописной буквы Г. На рис.4 представлены ДН для диполей с

плечами Г-образной формы, отличающихся друг от друга точкой, в которой выполнен поворот проводника на 90°.

Как видно из рассмотрения, наилучшей формой ДН обладает диполь, у которого участок диполя от центра диполя до поворота на 90° составляет долю, равную 0,41 длины плеча диполя. Такое соотношение частей плеча диполя естественна, поскольку токи, текущие по прилегающей к центру части плеча больше, чем токи, текущие по периферийной части плеча.

Диаграмма направленности в горизонтальной плоскости для кроссполяризационной (вертикальной) составляющей напряжённости электрического поля (рис.5) имеет вид восьмёрки. Нулевые уровни ДН направлены перпендикулярно к плоскости, в которой лежат плечи си мметрирующего устройства, а максимальные уровни — в плоскости плеч СУ. Форма ДН для вертикальной составляющей свидетельствует о том, что излучение вертикальной компоненты поля обусловлено противофазными токами, текущими по плечам СУ в противоположных направлениях.

На рис. 3 представлено распределение тока на излучающих и конструктивных элементах антенны. Следует отметить принципиальное отличие в распределении тока на плечах прямолинейного диполя и плечах диполя с 90° изгибом плеч. В плечах классического прямолинейного диполя распределение имеет вид стоячей волны тока. В плечах диполя с изгибом распределение имеет вид стоячей волны тока на ортогональной части плеча и вид смешанной волны на основной (исходной) части плеча.

Выводы

Выбором сечений поворота каждого плеча вибратора на 90 градусов относительно неизменной части плеча возможно создать антенну с диаграммой направленности, близкой к круговой, в плоскости вектора Е.

Теоретически достижимое отклонение формы диаграммы направленности от окружности составляет величину ±0,2 дБ.

Антенна конструктивно проста, обеспечивает удобное подключение фидера и предотвращает проявление антенного эффекта фидера за счет введения в конструкцию антенны симметрирующего устройства.

Антенна полезна для приёма сигналов курсо-глиссадных радиомаяков с целью подтверждения целостности системы посадки воздушных судов.

Целесообразно продолжить исследование характеристик данной антенны с целью обеспечения согласования её с линией питания и экспериментальные исследования.

Благодарности

Авторы выражают свою благодарность Фомину Д.Г. за его вклад в разработку макета антенны.

Литература

1. Annex 10 to the Convention on International Civil Aviation. Vol. 1. Radio Navigation Aids. Monreal (Canada), ICAO, 2006. 616 p.

2. Annex 10 to the Convention on International Civil Aviation. Aeronautical Telecommunications. Vol. 1. Radio Navigation Aids. 7th ed., Montreal (Canada), ICAO, 2018

3. Войтович Н. И.,Жданов Б. В. Способ лётных проверок наземных средств радиотехнического обеспечения полётов и устройства для его применения. Патент РФ на изобретение № 2 501 031 C2 позаявке 2011133133 от 05.08.2011. Опубликовано: 10.12.2013. Бюл. №34.

4. Фетисов В.С., Неугодникова Л.М., Адамовский В.В., Краснопёров Р.А. Беспилотная авиация: терминология, классификация, современное состояние. Под ред. В.С. Фетисова. Уфа: ФОТОН, 2014. – 217 с.

5. G.H. Brown, "The Turnstile Antenna", Electronics, April 1936, pp. 14-17.

6. Справочник по антенной технике: Справ. В 5 т. Т.1/Л.Д. Бахрах, Л.С. Бененсон, Е.Г. Зелкин и др; Под ред. Я.Н. Фельда, Е.Г.Зелкина. – М.: ИПРЖР, 1997.

7. X.L. Quan, and R.L. Li, "A broadband dual-polarized omnidirectional antenna for base stations", IEEE Trans. Antennas Propag., vol. 61, no. 2,pp. 943–947, Feb. 2013.

8. K. Wei, Z. Zhang, Z. Feng et al., "A MNG-TL loop antenna array with horizontally polarized omnidirectional patterns", IEEE Trans. Antennas Propag., vol. 60, no. 6, pp. 2702-2710, 2012.

9. Z. D. Wang, Y. Z. Yin, X. Yang, J. J. Wu, "Design of a wideband horizontally polarized omnidirectional antenna with mutual coupling method", IEEE Trans. Antennas Propagat., vol. 63, no. 7, pp. 3311-3316, Jul. 2015.

10. Shixian Chen, Yufa Sun, Dong Zhou, "A wideband omnidirectional horizontally polarized antenna

for wireless applications", Microwave and Millimeter Wave Technology (ICMMT) 2016 IEEE International Conference on, vol. 2, pp. 713-715, 2016.

11. Hatim Bukhari, Kamal Sarabandi, "Miniaturized omnidirectional horizontally polarized antenna", IEEE Trans. On Antennas Propag, vol. 63, no. 10, pp. 4280-4285, Oct. 2015.

12. G. Jiang, C. Guo, "A broadband horizontally polarized omnidirectional antenna array consisting of four corrugated TSA elements", 2016 CIE International Conference on Radar, pp. 1-5, October 2016.

13. H. Liu, Y. Liu, W. Zhang, S. Gao, "An ultra-wideband horizontally polarized omnidirectional circular connected Vivaldi antenna array", IEEE Transactions on Antennas and Propagation, vol. 65, no. 8, pp. 4351-4356, August 2017.

14. C.A. Balanis, Antenna theory analysis and design, New Jersey, 2005. – 1070 p.

15. R. E. Collin, Antennas and Radiowave Propagation. New York, NY, USA: McGraw-Hill, 1985.

16. Peng Luo, Yuehui Cui, RongLin Li, "Novel multiband/broadband horizontally polarized omnidirectional antennas", Antennas and Propagation (APSURSI) 2016 IEEE International Symposium on, pp. 1795-1796, 2016.

17. Фомин Д.Г., Войтович Н.И. Магнитный датчик контроля АФР антенны. Труды 28 международной конференции "Микроволны и телекоммуникационные технологии (КрыМиКо 2018)" Севастополь, сентябрь 9-15, 2018.

18. Carter, P.S.: "Wide band antenna", US patent № 2258406, 1938 г.

19. H. Hertz. Uber sehrschnelleelektrischeSchwingunges. Wied. Ann., 31, 421, 1887.

20. Герц Г.Р. 50 лет волн Герца (сборник избранных работ Г. Герца. Под ред. Аркадьева В.К.). М.-Л.: АН СССР, 1938.

21. Бузов А.Л., Сподобаев Ю.М., Филиппов Д.В. Юдин В.В. Электродинамические методы анализа проволочных антенн. М.: Радио и связь. – 2000, - 153 с.

22. Ершов А.В. Широкополосная вибраторная антенна для многоканального радиовешания. Кандидатская диссертация. Челябинск.: ЮУрГУ. – 2004.

References

1. Annex 10 to the Convention on International Civil Aviation. Vol. 1. Radio Navigation Aids. Monreal (Canada), ICAO, 2006. 616 p.

2. Annex 10 to the Convention on International Civil Aviation. Aeronautical Telecommunications. Vol. 1. Radio Navigation Aids. 7th ed., Montreal (Canada), ICAO, 2018

3. Voytovich N. I., Zhdanov B. V. Sposob lyotny'x proverok nazemny'x sredstv radiotexnicheskogo obespecheniya polyotov i ustrojstva dlya ego primeneniya. Patent RF na izobretenie № 2 501 031 S2 pozayavke 2011133133 ot 05.08.2011. Opublikovano: 10.12.2013. Byul. №34.

4. Fetisov V.S., Neugodnikova L.M., Adamovskij V.V., Krasnopyorov R.A. Bespilotnaya aviaciya: terminologiya, klassifikaciya, sovremennoe sostoyanie. Pod red. V.S. Fetisova. Ufa: FOTON, 2014. – 217 s.

5. G.H. Brown, "The Turnstile Antenna", Electronics, April 1936, pp. 14-17.

6. Spravochnik po antennoj texnike: Sprav. V 5 t. T.1/L.D. Baxrax, L.S. Benenson, E.G. Zelkin i dr; Pod red. Ya.N. Fel'da, E.G.Zelkina. – M.: IPRZhR, 1997.

7. X.L. Quan, and R.L. Li, "A broadband dual-polarized omnidirectional antenna for base stations", IEEE Trans. Antennas Propag., vol. 61, no. 2,pp. 943–947, Feb. 2013.

8. K. Wei, Z. Zhang, Z. Feng et al., "A MNG-TL loop antenna array with horizontally polarized omnidirectional patterns", IEEE Trans. Antennas Propag., vol. 60, no. 6, pp. 2702-2710, 2012.

9. Z. D. Wang, Y. Z. Yin, X. Yang, J. J. Wu, "Design of a wideband horizontally polarized omnidirectional antenna with mutual coupling method", IEEE Trans. Antennas Propagat., vol. 63, no. 7, pp. 3311-3316, Jul. 2015.

10. Shixian Chen, Yufa Sun, Dong Zhou, "A wideband omnidirectional horizontally polarized antenna for wireless applications", Microwave and Millimeter Wave Technology (ICMMT) 2016 IEEE International Conference on, vol. 2, pp. 713-715, 2016.

11. Hatim Bukhari, Kamal Sarabandi, "Miniaturized omnidirectional horizontally polarized antenna", IEEE Trans. On Antennas Propag, vol. 63, no. 10, pp. 4280-4285, Oct. 2015.

12. G. Jiang, C. Guo, "A broadband horizontally polarized omnidirectional antenna array consisting of four corrugated TSA elements", 2016 CIE International Conference on Radar, pp. 1-5, October 2016.

13. H. Liu, Y. Liu, W. Zhang, S. Gao, "An ultra-wideband horizontally polarized omnidirectional circular connected Vivaldi antenna array", IEEE Transactions on Antennas and Propagation, vol. 65, no. 8, pp. 4351-4356, August 2017.

14. C.A. Balanis, Antenna theory analysis and design, New Jersey, 2005. – 1070 p.

15. R. E. Collin, Antennas and Radiowave Propagation. New York, NY, USA: McGraw-Hill, 1985.

16. Peng Luo, Yuehui Cui, RongLin Li, "Novel multiband/broadband horizontally polarized omnidirectional antennas", Antennas and Propagation (APSURSI) 2016 IEEE International Symposium on, pp. 1795-1796, 2016.

17. Fomin D.G., Voytovich N.I. Magnitny'j datchik kontrolya AFR antenny'. Trudy' 28 mezhdunarodnoj konferencii "Mikrovolny' i telekommunikacionny'e texnologii (Kry'MiKo 2018)" Sevastopol', sentyabr' 9-15, 2018.

18. Carter, P.S.: "Wide band antenna", US patent № 2258406, 1938.

19. H. Hertz. Uber sehrschnelleelektrischeSchwingunges. Wied. Ann., 31, 421, 1887.

20. Gerc G.R. 50 let voln Gerca (sbornik izbranny'x rabot G. Gerca. Pod red. Arkad'eva V.K.). M.-L.: AN SSSR, 1938.

21. Buzov A.L., Spodobaev Yu.M., Filippov D.V. Yudin V.V. E'lektrodinamicheskie metody' analiza provolochny'x antenn. M.: Radio i svyaz'. — 2000, — 153 s.

22. Ershov A.V. Shirokopolosnaya vibratornaya antenna dlya mnogokanal'nogo radioveshaniya. Kandidatskaya dissertaciya. Chelyabinsk.: YuUrGU. – 2004.

ВОЙТОВИЧ Вадим Вадимович, инженер-исследователь, ООО «Конструкторское Бюро «ЭКРАН» имени М.А. Шильмана». 454080, г. Челябинск, ул. Энтузиастов, 26Б. E-mail: vadimka.voytovich@mail.ru

VOYTOVICH Vadim, research engineer, LLC "Design Bureau "EKRAN" named after M.A. Shilman". 26B, Enthusiasts st., Chelyabinsk, Russia, 454080. E-mail: vadimka.voytovich@mail.ru

ПЕТРАШ Юрий Валерьевич, инженер-исследователь, ООО «Конструкторское Бюро «ЭКРАН» имени М.А. Шильмана». 454080, г.Челябинск, ул. Энтузиастов, 26Б. E-mail: yurapetrash111@gmail.com

PETRASH Iyurii, research engineer, LLC "Design Bureau "EKRAN" named after M.A. Shilman". 26B, Enthusiasts st., Chelyabinsk, Russia, 454080. E-mail: yurapetrash111@gmail.com

БЕЛОУСОВ Макар Михайлович, инженер-исследователь, ООО «Конструкторское Бюро «ЭКРАН» имени М.А. Шильмана». 454080, г.Челябинск, ул. Энтузиастов, 26Б. E-mail: makarbel84@gmail.com

BELOUSOV Makar, research engineer, LLC "Design Bureau "EKRAN" named after M.A. Shilman". 26B, Enthusiasts st., Chelyabinsk, Russia, 454080. E-mail: makarbel84@gmail.com

ЮНГАЙТИС Екатерина Михайловна, младший научный сотрудник, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: jungaitis92@gmail.ru

IUNGAITIS Ekaterina, junior researcher, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 76, Lenin prospect, Chelyabinsk, 454080, Russia. E-mail: jungaitis92@gmail.ru

ЕРШОВ Алексей Валентинович, кандидат технических наук, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: eav@list.ru

ERSHOV Aleksey, PhD in Engineering sciences, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 76, Lenin prospect, Chelyabinsk, 454080, Russia. E-mail: eav@list.ru

ВОЙТОВИЧ Николай Иванович, доктор технических наук, профессор, заведующий кафедрой конструирования и производства радиоаппаратуры, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г.Челябинск, пр. им. В.И. Ленина, 76. E-mail: voytovichni@mail.ru

VOYTOVICH Nikolay, Doctor of Technical Sciences, Professor, Head of the Department of Design and Production of Radio Equipment, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 76, Lenin prospect, Chelyabinsk, 454080, Russia. E-mail: voytovichni@mail.ru

УДК 004.738.5 Вестник УрФО № 4(38) / 2020, с. 44–54

Пономарёв К.Ю., Захаров А.А.

DOI: 10.14529/secur200404

МЕТОДЫ РАЗГРАНИЧЕНИЯ ДОСТУПА В СЕТЯХ ИНТЕРНЕТА МЕДИЦИНСКИХ ВЕЩЕЙ НА ОСНОВЕ АТРИБУТИВНЫХ МОДЕЛЕЙ

Термином «Интернет медицинских вещей» («InternetofMedicalThings», «IoMT») называют совокупность устройств и технологий удаленного мониторинга состояния здоровья пациентов с использованием носимых устройств. Одной из проблем, затрудняющих массовое внедрение технологий IoMTявляетсяресурсоёмкая защита пользовательских сведений при передаче информации по незащищенным каналам связи и её хранение в облачных системах.Ставшие уже классическими технологии и методызащиты Интернет-ресурсов и систем массового обслуживанияне подходят в том случае, когда речь идёт о миллионах устройств IoMT, по такимпараметрам как:низкая вычислительная мощность, нехватка памяти, ограниченная емкость батареи питания и др. В работе исследуются возможности использования атрибутивного шифрования ABE («Attribute-basedencryption») для защиты персонифицированной информации всетях IoMT. Изучаются вопросыконфиденциальности данных пациента при передаче и хранении информации в облаке, менеджмент криптографических ключей и контроль за распространением данных. Предлагаются алгоритмы для приемлемого защищенного решения. Предложен фреймворк для обработки данных пациентов с портативных диагностических устройств с использованием методов атрибутивного шифрования. Приведены результаты нагрузочного тестирования прототипа.

Ключевые слова: *телемедицина, электронные персональные медицинские карты, авторизация, интернет вещей, атрибутивный контроль доступа.*

Исследование выполнено при финансовой поддержке гранта: РФФИ и Тюменской области в рамках научного проекта № 20-47-720005 и гранта РФФИ 22/2020.

Ponomarev K.Y., Zaharov A.A.

ACCESS CONTROL METHODS FOR INTERNET OF MEDICAL THINGS NETWORKS BASED ON ATTRIBUTE MODELS

The term «Internet of Medical Things» (IoMT) refers to a set of devices and technologies for remote monitoring of patients' health using wearable devices. One primary problem with patient's data is ensuring privacy and resource intensive protection when it is transmitted over open communication channels and stored in cloud systems. However, when it comes to millions of IoT devices, technologies that have already become classic for Internet resources are not suitable in many aspects at once: low computing power, out of memory, limited battery capacity and etc. The work considered Attribute-based encryption for ensuring security of personified data in IoMT networks. Also, the research studied the issues of patient's data confidentiality in cloud systems, management of cryptographic keys and data sharing control. The algorithms for effective and secure solution were proposed. We have proposed a framework for processing patient data from portable diagnostic devices using ABE methods. The results of load testing of the prototype are presented too.

Keywords: *telemedicine, personal health records, authorization, internet of things, attribute-based access control.*

В современном мире время взаимодействиеврача и пациента ограничено, что обусловливает необходимость диагностировать и определять стратегию лечения в кратчайшие сроки, не теряя при этом качество. Это требует внедрения в практику здравоохранения передовых научных разработок, в том числе достижений в области информационно-коммуникационных технологий, которые стимулируют развитие новых концепций персонализированного здравоохранения. Отметим, что процесс перехода от бумажных носителей к цифровым, делает необходимым переход от управления бумагами к управлению данными, что требует изменения стандартов работы с медицинской информацией.

В настоящее время наиболее распространенными технологиями работы с медицинской информацией являются **электронные медицинские карты (ЭМК)**, представляющие совокупность электронных персональных медицинских записей (ЭПМЗ), относящихся к пациенту, собираемых, хранимых и используемых в рамках одной медицинской организации. Термин ЭМК является аналогом международного термина ElectronicMedical Record (EMR). Отвечая на современные требования к организации распределенной инфраструктуры медицинской помощи,в России вместо стандарта ГОСТ Р 52636-2006 «Информатизация здоровья. Электронная медицинская карта. Электронная медицинская карта, используемая в медицинской организации», разрабатываются два дополнительных стандарта: ГОСТ Р «Информатизация здоровья. Электронная медицинская карта. Интегрированная электронная медицинская карта» и ГОСТ Р «Информатизация здоровья. Электронная медицинская карта. Персональная электронная медицинская карта» [1].

Деление понятия «Электронная медицинская карта» на 3 новых функциональных слоя обеспечит совместное использование данных из медицинских записей,их единообразное пониманиеи трактовку не только сотрудниками различных медицинских организаций, но и даст возможность пациенту проявить заботу о собственном здоровье. Такая организация работы с медицинской информацией характеризуется термином

5П-медицина, отражающим следующие основополагающие принципы: персонализация, предикция, превентивность, парсипативность и прецизионность [2,3]. При этом, хотя реализаций полного спектра 5П в полном объемепока не существует, запрос на новые подходы к сохранению своего здоровья (персонализация, предикция, превентивность) уже сформировал на основе понятия «Интернет вещей» (IoT) термин «Интернет медицинских вещей» (от англ. «Internet of MedicalThings», «IoMT»), как совокупность устройств и технологий удаленного мониторинга состояния здоровья с использованием носимых устройств [4].

СистемыIoMT могут использоваться для объединения доступных медицинских ресурсов и предоставления умных комплексных медицинских услуг, например, в процессе реабилитации пожилых пациентов после инсульта, мониторинга состояния здоровья пациентов с хроническими заболеваниями, в том числе пациентов, живущих в удаленных местах [5-6].

Технологии на базе IoMTиспользуют портативные медицинские устройства, объединённые в беспроводную нательную сеть WBAN (англ. WirelessBodyAreaNetwork) [7] для сбора медицинских данных пациентов и записи информации в электронную персональную медицинскую запись (ЭПМЗ). Совокупность электронных персональных медицинских записей (ЭПМЗ), поступивших из различных источников и относящихся к одному человеку, который осуществляет сбор, управление иназначение права доступа к ЭПМЗ определяет **персональную электронная медицинскую карта (ПЭМК)** – аналог международного термина PersonalHealthRecord (PHR) [8].

ПЭМК - являются основой для создания систем персонализированной медицины, находящихся в облачном защищенном хранилище. Идея, лежащая в основе таких систем, заключается в том, что пользователь хранит собственную ПЭМК и регулирует к ней доступ персоналу медицинских учреждений, сотрудникам страховых компаний, родственникам. Это актуально в современных условиях, когда пользователь может быть связан с большим количеством медицинских организаций, каждая из которых ведёт свою собственную базу пациентов и высокой мобильностью граждан (переезды внутри одного города или в рамках всей страны). Отметим, что в качестве поставщика данных ПЭМК могут выступать сами пациенты, медицинские информационные системы лечебных учреждений, а также портативные диагностические устройства в автоматическом режиме собирающие и передающие данные, например, в облако дляих анализа и хранения.

Совокупность электронных персональных медицинских записей (ЭПМЗ), относящихся к одному человеку, собираемых, передаваемых и используемых несколькими медицинскими организациями формируют **Интегрированную электронную медицинскую карту (ИЭМК)**[9].

Используя данныеИЭМК и ПЭМК можно выявить закономерности изменений состояния здоровья, особенности течения заболеваний и оценить качество медицинского обслуживания. Для извлечения валидной информации из неструктурированных данных ИЭМК и ПЭМК выявления характерных категорий пациентов используются методы data mining иBig Data[10 - 11].

Отметим, что поскольку IoMT тесно интегрирован с ПЭМК и ИЭМК, сетями IoT, аналитическими приложениями и сервисами обработки данных, то в сетях IoMT пристальное внимание должно уделяться разграничению доступа к данным и их конфиденциальности при передаче по открытой сети [12,13], а также хранению в облачном хранилище [14,15]. Поскольку пациент имеет минимальный контроль над своими данными, после того как они были переданы в облачное хранилище, тоэти данные подвержены таким угрозам нарушения конфиденциальности как инсайд со стороны облачного провайдера или администратора приватного облака, потери данных, влияния других виртуальных сред и наличия небезопасных интерфейсов доступа к данным. Отметим также, что на сетевом уровне взаимодействия между устройствами, облаками и промежуточными узлами обычно используются протоколы Wi-Fi, BLE, ZigBee [16], которые уязвимы к таким атакам как «человек посередине» или «повтор сообщений».

Одним из эффективных методов, обеспечивающих безопасность и хранение данных ПЭМК, является криптографическая защита информации. Принципиально важно, что симметричные алгоритмы шифрования менее ресурсоёмки и, следовательно, больше подходят для IoT устройств с низким энергопотреблением, но они являются уязвимыми с точки зрения механизмов обмена ключами.

Перечислим основные свойства систем

ПМЭК с точки зрения информационной безопасности.

• Конфиденциальность: сведения должны быть защищены как в процессе передачи, так и при хранении в облачном хранилище. Необходима защита данных от посторонних наблюдателей в открытой сети, самого облачного провайдера или злоумышленников, нарушивших его целостность.

• Ориентированность на пациента: пользователь имеет полный контроль над своими данными и регулирует политики доступа к ним. С точки зрения врача это означает, что при обращении новый пациент может предоставить доступ ко всей своей истории болезни, включая все детали заключений врачей и все предыдущие анализы.

• Делегирование и отзыв прав: пользователь имеет возможность отозвать доступ у кого-либо к своим сведениям или делегировать право на управление своими записями кому-либо (например, родственникам). Также стоит отметить такой момент, как доступ персонала скорой помощи к пользовательским сведениям в чрезвычайных ситуациях.

В традиционным подходе к защите информации криптосистемам необходимо явно указать получателя данных (например, используя его сертификат открытого ключа), но это неприменимо в рассматриваемой медицинской прикладной области: пациент, загружая сведения, может не знать конкретных потребителей информации. Таким образом, современные средства защиты на основе симметричных и асимметричных криптосистем малоэффективны при работе с ПЭМК.

Перспективы безопасного интернета медицинских вещей обсуждаются в работе [17-21]. Авторы обсуждают подходы к решению таких проблем IoT eHealth, как управление данными, масштабируемость, правила, совместимость интерфейсов устройств IoMIT-сеть-человек, а также безопасность и защиту конфиденциальности объектов и пользователей. В работе [22]авторы в качестве эффективного метода защиты пользовательских сведений предложили алгоритмы атрибутивного шифрования - ABE («attributebasedencryption»). Их идея заключается в том, что в криптосистеме с открытым ключом в качестве публичного ключа используется набор открытых параметров - атрибутов субъекта доступа. За генерацию соответствующих приватных ключей ответственен выделенный атрибутивный центр. Использование таких алгоритмов для защиты ЭМК позволяет решить множество проблем, описываемых разработчиками системперсонализированной медицины: конфиденциальность данных пациента при хранении в облаке, упрощенные механизмы менеджмента криптографических ключей, контроль за распространением данных самим пациентом.

1. Шифрование на основании атрибутов

Шифрование на основе атрибутов берёт своё начало из схем личностного шифрования («Identity-basedencryption»), которые являются разновидностью криптосистем с открытым ключом[23]. В роли открытого ключа в них используются параметры или атрибуты самого пользователя, например, адрес электронной почты. Каждый такой открытый параметр отображается в открытый криптографический ключ, а для расшифрования сообщений, сформированных с помощью этого ключа в центре генерации ключей, формируется соответствующий закрытый ключ [24].

В работе [25]набор открытых параметров шифртекста соответствует структуре доступа к данным, а набор открытых параметров пользователя – его атрибутам, на основании которых центр генерации ключей формирует ему секретный ключ. Пользователь, имеющий определённый закрытый ключ, может расшифровать шифртекст, тогда и только тогда, когда структура доступа соответствует атрибутам пользователя. В дальнейшем исследователи разрабатывали различные способы соответствия между этими наборами параметров, например, структура доступа может представлять собой булевскую формулу над пользовательскими атрибутами.

Основная сущность в ABE-схемах - атрибутивный центр («AttributeAuthority»). Он несёт ответственность за формирование и управление криптографическими ключами, верификацию атрибутов.

Существуют два вида схем атрибутивного шифрования – «Key-Policy» (KP-ABE) и «Ciphertext-Policy» (CP-ABE).Их основное отличие заключается в том, где располагается структура доступа к данным: в первом случае – в секретном ключе пользователя, во втором – в шифртексте. CP-ABE криптосистемы принято считать более гибкими и практическими полезными. Любая такая схема предоставляет следующие функции: формирования открытого и секретного мастер ключа; генерации приватного ключа на основании множества атрибутов; формирования шифртекста на основе открытого текста и структуры до-

ступа; расшифрования на основании шифртекста, структуры доступа и секретного пользовательского ключа.

2. Платформа обработки и хранения медицинских данных

Рассмотрим IoMT платформу, состоящую из следующих основных сущностей:

• Облачное хранилище медицинских данных (*Cloud*): хранит записи в разрезе пациентов, предоставляет API для доступа к медицинским сведениям.

• Атрибутивный центр (A*ttributeAuthority, AA*): служит центром регистрации для всех субъектов платформы - пациентов, врачей, IoT устройств, различных сервисов обработки и анализа данных. Хранит атрибуты для каждого из них, генерирует ключи схемы атрибутивного шифрования. Пациенты указывают политики доступа к своим данным в облачных хранилищах в виде атрибутивных правил. Атрибутивный центр имеет общий секретный ключ с каждым из зарегистрированных субъектов.

• Персональное дистанционное устройство (ПДУ, *Device*): собирает или агрегирует медицинские показатели с других устройств пациента, отправляет на дальнейшую обработку в облачное хранилище. Пациент имеет возможность зарегистрировать свои ПДУ в атрибутивном центре.

• Сервис генерации токенов (Token Generation Service, TGS): необходим для проверки прав доступа к API облачного хранилища.

Пошагово опишем процессы передачи данных - показателей жизнедеятельности пациента - в облако и их обработки.

1. Пациент выполняет процедуру регистрации для себя и своих ПДУ в атрибутивном центре. В итоге для каждого ПДУ будет указан список атрибутов, используемый для генерации приватного ключа, и секретный ключ, используемый при аутентификации в *АЦ*. Для верификации атрибутов возможен контроль со стороны медицинского персонала.

2. Пациент указывает в *АЦ* какие атрибутивные структуры доступа следует использовать при доступе к его данным. В дальнейшем для простоты будем считать, что используются только операции чтения и записи.

3. Пациент конфигурирует свои ПДУ: он должен указать им ключ доступа к атрибутивному центру, созданный при регистрации на первом шаге.

4. При старте работы ПДУ запрашивает в атрибутивном центре приватный ключ *ABE* схемы, который будет использоваться для авторизации в облачном хранилище. Для аутентификации и авторизации в *AA* используется ключ доступа, указанный на предыдущем шаге.

5. ПДУ инициирует запрос в *Cloud* на передачу показаний жизнедеятельности пациента.

6. ПДУ, облачное хранилище и *TGS* совместно выполняют протокол атрибутивного контроля доступа с целью проверки прав доступа на запись сведений.

7. В случае успешной проверки в хранилище происходит запись данных пациента в зашифрованном виде, такие образом с помощью *ABE* сведения будут защищены от облачного провайдера или от злоумышленника в случае его компрометации.

8. Автоматизированные сервисы обработки данных также получают от АЦ приватный ключ схемы атрибутивного шифрования. Они обращаются в API облачного хранилища за данными по пациентам, выполняют протокол атрибутивного контроля доступа с целью проверки прав доступа на чтение. Предполагается, что эти сервисы могут выявлять возможные отклонения в данных пациента, и в критических случаях уведомляют об этом пациента и его лечебное учреждение.

На основании описанных процессов можно выделить следующие требования к механизмам авторизации и аутентификации в рассматриваемой IoMT платформе. Эти требования соответствуют свойствам ЭМК, указанным ранее.

1. Пациент должен самостоятельно определять политики доступа на различные операции со своими данными в облаке, например, на запись и чтение. Для проверки прав доступа к данным пациента через API облачного хранилища должны использоваться указанные пациентом политики доступа.

2. Облачное хранилище знает, какому пациенту принадлежат передаваемые данные, однако не имеет к ним доступа, поскольку медицинские данные пациентов хранятся в зашифрованном виде.

3. Передача информации в открытой сети должна идти по защищенному каналу связи.

Внедрение методов атрибутивного контроля доступа и алгоритмов атрибутивного шифрования повышает эффективность механизмов безопасности IoMT платформ. Отметим, следующие положительные стороны предлагаемого подхода:

• используемая атрибутивная модель доступа является наиболее подходящей для современных динамичных сетей Интернета вещей и позволяет использовать гибкие и гранулированные политики доступа;

• *ABE* используется как для проверки прав доступа, так и для защиты информации в процессах её передачи по открытой сети и хранении в облаке;

• за счёт применения *ABE* реализуется механизм единого входа (SingleSignOn), когда приватный ключ, полученный от атрибутивного центра, может использоваться для доступа к различным облачным ресурсам;

• за счёт применения *ABE* упрощаются механизмы управления ключами, т.к. отправителю и получателю не нужно выполнять процедур по предварительному обмену ключами.

количество запросов к платформенным сервисам. Методика тестирования заключалась в выполнении процесса передачи данных по представленному ранее сценарию и измерении времени, прошедшего с момента отправки запроса от ПДУ до момента получения ответа на запрос. Данная величина включает в себя время, необходимое запрашиваемым сервисам на обработку запроса, в том числе на запросы к другим сервисам. Мы будет называть её временем отклика или временем выполнения запроса. Тестовый стенд был развёрнут на ресурсах платформы для облачных вычислений «Яндекс.Облако» (*http://cloud.yandex.ru*). Использовались виртуальные машины и диски сервиса *ComputeCloud*, их список приведён в таблице ниже. Все машины располагались в одной зоне доступно-

Рис. 1. Схема взаимодействия внутри IoMT платформы

Табл. 1

Характеристики виртуальных машин тестового стенда

Название	Количество виртуальных ядер (*vCPU*)	Гарантированная доля *vCPU*	Размер оперативной памяти, ГБ (*RAM*)	Размер *HDD* диска, ГБ
abe-vm1	2	5%	1	8
abe-vm2	2	100%	2	8
abe-vm3	2	100%	2	5

3. Нагрузочное тестирование прототипа IoMT платформы

В данной части будут представлены результаты нагрузочного тестирования прототипа IoMT платформы. Целью является выяснение возможности применения представленной модели в реальных системах Интернета вещей, для которых характерно большое

сти (*ru-central1-c*), то есть находились в одном дата-центре. На всех машинах была установлена операционная система *Ubuntu 18.04 LTS*.

Существенное влияние на время выполнения алгоритмов атрибутивного шифрования оказывает количество атрибутов. Поэтому в каждом эксперименте их количество постепенно увеличивалось, на каждый размер

множества атрибутов запускался тестовый сценарий. Также тестовые сценарии вначале запускались в одном потоке, потом параллельно в нескольких - с целью симуляции нагрузки на сервисы. На измеряемое время отклика могли влиять следующие факторы:

• на тестовом стенде размер коллекции в БД для хранения списка зарегистрированных устройств состоит из десятка записей, в реальных системах - это сотни тысяч записей, затраты на поиск в БД остаются неучтёнными в данном тесте, так как на практике это зависит от выбора конкретной СУБД и архитектуры масштабирования;

• в прототипе используется стороннее ПО для выполнения алгоритмов атрибутивного шифрования, что требует запросов к файловой системе, которые могут вносить задержки в измеряемое время.

ности и эффективности. С целью проверки возможностей подсистемы при горизонтальном масштабировании мы увеличивали количество экземпляров сервисов. В системах Интернета вещей масштабируемость сервисов и приложений имеет критическое значение, так как именно она обеспечивает доступность и позволяет выдерживать большие нагрузки. Для балансировки нагрузки использовался веб-сервер *nginx* с простым циклическим алгоритмом (*roundrobin*) балансировки.

Результаты нагрузочных экспериментов сильно зависят от используемой атрибутивной криптосистемы, деталей реализации, используемых языков программирования, фреймворков, СУБД и систем хранения данных. Поэтому они могут сильно отличаться в каждой конкретной информационной системе. Тем не менее, повысить эффективность

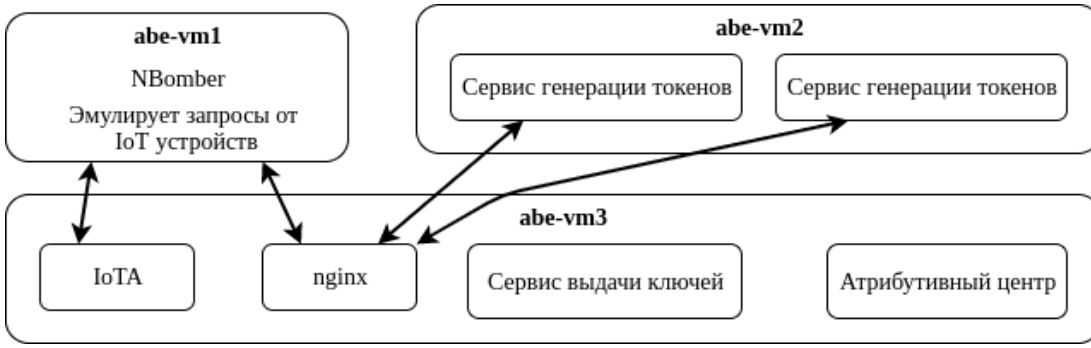


Рис. 2. Схема стенда для тестирования IoMT платформы

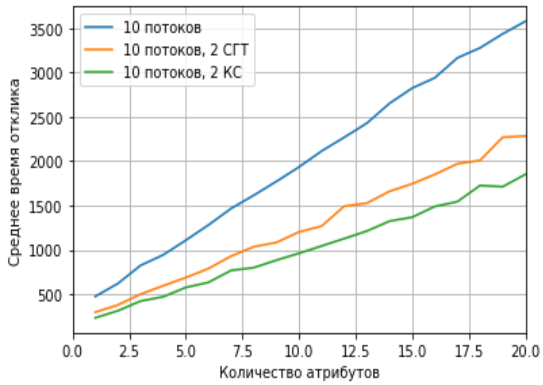


Рис. 3. Среднее время отклика при тестировании сервисов контроля доступа

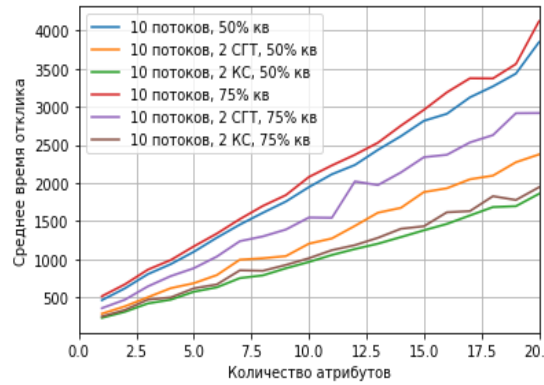


Рис. 4. Квантили времени отклика при тестировании сервисов контроля доступа

Из графиков становится ясным, что время выполнения запроса имеет практически линейную зависимость от размера множества атрибутов, это явление характерно для большинства схем атрибутивных криптосистем. Схемы *ABE* с таким свойством более распространены, а значит, имеют больше практически полезных свойств и лучше изучены, однако они ограничены в плане производительности системы можно масштабируя сервисы. При выборе того, у каких сервисов подсистемы атрибутивного контроля доступа необходимо увеличивать количество одновременно работающих экземпляров, следует учитывать следующие факторы:

• какие сервисы выполняют самые трудоёмкие криптографические операции схемы атрибутивного шифрования;

• какие сервисы испытывают большую нагрузку со стороны пользователей и устройств Интернета вещей;

• время жизни сессии взаимодействия между ПДУ и облаком, от этого зависит, как часто будет выполняться протокол атрибутивного контроля доступа, и соответственно нагрузка на сервисы генерации токенов;

• время жизни приватных криптографических ключей схемы *ABE*, от этого зависит нагрузка на сервисы раздачи ключей и атрибутивный центр.

4. Заключение

Разработка новых механизмов и моделей безопасности для систем персонализированного здравоохранения и сетей Интернета вещей является актуальной научной задачей. В данной статье была рассмотрена методы атрибутивного контроля доступа к ПЭМК пациентов для систем Интернета медицинских вещей. Нами были представлены: архитектурная модель платформы Интернета медицинских вещей, результаты нагрузочного тестирования прототипа. Непосредственно из работы следует необходимость в разработке следующих методов:

• системы атрибутивного контроля для платформ Интернета вещей с несколькими атрибутивными центрами - иерархическими, децентрализованными - и методы их применения на практике;

• разработка способов интеграции атрибутивных моделей в существующие платформы и решения;

• способность представленной модели противостоять атакам типа «отказ в обслуживании», или DDOS атакам;

• изучение возможностей дальнейшей эффективной работы и защиты пользовательских данных при компрометации атрибутивного центра;

• методы и протоколы отзыва атрибутов и секретных ключей схемы шифрования на основании атрибутов;

• производительность и эффективность схем атрибутивного шифрования на устройствах Интернета вещей.

Литература

1. Проект ГОСТ Электронная медицинская карта. Термины и определения.URL: http://portal.egisz.rosminzdrav.ru/materials/310 (дата обращения: 01.11.2020)

2. Щербо С. Н., Щербо Д. С. Медицина 5П: прецизионная медицина //Медицинский алфавит. – 2015. – Т. 4. – №. 18. – С. 5-10.

3. Zakharov A., Potapov A., Zakharova I., Kotelnikov A., Panfilenko, D. Infrastructure of the Electronic Health Record Data Management for Digital Patient Phenotype Creating. // 7th Scientific Conference on Information Technologies for Intelligent Decision-Making Support (ITIDS 2019). – Atlantis Press. -2019.

4. Joyia G. J. et al. Internet of Medical Things (IOMT): applications, benefits and future challenges in healthcare domain //J Commun. – 2017. – Т. 12. – №. 4. – С. 240-247.

5. ZakharovA. A., Potapov A. P., Zakharov, I. G., Olennikov E. A. Telemetric Medical System to Support Cardiological Screening. // In 2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE). – IEEE. - 2018. - С. 116-120.

6. Hassan M. K. et al. A Hybrid Real-time remote monitoring framework with NB-WOA algorithm for patients with chronic diseases //Future Generation Computer Systems. – 2019. – Т. 93. – С. 77-95.

7. Khan J. Y. et al. Wireless body area network (WBAN) design techniques and performance evaluation //Journal of medical systems. – 2012. – Т. 36. – №. 3. – С. 1441-1457.

8. ISO/TR 20514:2005 «Health informatics – Electronic health record – Definition, scope and context». URL: https://www.iso.org/standard/39525.html (дата обращения 20.10.2020)

9. Зарубина Т.В., Швырев С.Л., Соловьев В.Г., Раузина С.Е., Родионов В.С., Пензин О. В., Сурин М. Ю. // Интегрированная электронная медицинская карта: состояние дел и перспективы. Врач и информационные технологи. -2016. - № 2.

10. Gehrmann,S., Dernoncourt F., Li Y., Carlson E. T., Wu J. T., Welt J., Celi, L. A. Comparing deep learning and concept extraction based methods for patient phenotyping from clinical narratives// PloS one. – 2018.

11. Zakharov A., Kotelnikov A., Potapov A., Panfilenko D., Gayduk P. Information and Analytical Support for Biomedical Research in the Field of the Cardiovascular Disease Risk Prediction. // 8th Scientific Conference on Information Technologies for Intelligent Decision-Making Support (ITIDS 2020). - Atlantis Press. - 2020.

Исследование выполнено при финансовой поддержке Минобрнауки России (Грант ИБ).

12. Masood I. et al. Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure //Wireless Communications and Mobile Computing. – 2018.

13. Kołodziej J. et al. Ultra Wide Band Body Area Networks: Design and Integration with Computational Clouds //High-Performance Modelling and Simulation for Big Data Applications. – Springer, Cham, 2019. – C. 279-306.

14. Kennedy Edemacu, Hung Kook Park, Beakcheol Jang, Jong Wook Kim. Privacy Provision in Collaborative Ehealth With Attribute-Based Encryption: Survey, Challenges and Future Directions //IEEE Access. - 2019. – 7.

15. Li M. et al. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings //International conference on security and privacy in communication systems. – Springer, Berlin, Heidelberg, 2010. – C. 89-106.

16. Sundaravadivel P., Kougianos E., Mohanty S. P., Ganapathiraju, M. K. Everything you wanted to know about smart health care: Evaluating the different technologies and components of the Internet of Things for better health. // IEEE Consumer Electronics Magazine. -2017. - 7(1), - C.18-28.

17. Farahani B. et al. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare //Future Generation Computer Systems. – 2018. – T. 78. – C. 659-676.

18. Лебедев Г.С., Шадеркин И.А., Фомина И.В., Лисненко А.А., Рябков И.В., Качковский С.В., Мелаев Д.В. ИНТЕРНЕТ МЕДИЦИНСКИХ ВЕЩЕЙ: ПЕРВЫЕ ШАГИ ПО СИСТЕМАТИЗАЦИИ // Журнал телемедицины и электронного здравоохранения. - 2017. - №3 (5).

19. Минаев Антон Андреевич, Купер Дмитрий Витальевич, Иващенко Антон Владимирович Современные тенденции по реализации распределенной медицинской диагностики на базе Интернета вещей // Известия Самарского научного центра РАН. - 2016. - №4-4.

20. Бухарев Д.А., Вагин С.В., Соколов А.Н. Защита устройств интернета вещей от mirai-подобных вирусных программ-червей //Вестник УрФО. Безопасность в информационной сфере. – 2018. – №. 4. – С. 11-19.

21. Маслова М.А. Принципы безопасности интернета вещей //Вестник УрФО. Безопасность в информационной сфере. – 2018. – №. 3 (29). – С. 38-42.

22. Wang C., Liu X., Li W. Design and implementation of a secure cloud-based personal health record system using ciphertext-policy attribute-based encryption //International Journal of Intelligent Information and Database Systems 4. – 2013. – Т. 7. – №. 5. – С. 389-399.

23. A. Shamir. Identity-based cryptosystems and signature schemes. // Workshop on the theory and application of cryptographic techniques. – Springer, Berlin, Heidelberg. - 1984. – С. 47-53.

24. D. Boneh. M. Franklin. Identity-based encryption from the Weil pairing. //Annual international cryptology conference. - Springer, Berlin, Heidelberg. - 2001. – С. 213-229.

25. A. Sahai, and B. Waters. Fuzzy identity-based encryption. //Annual International Conference on the Theory and Applications of Cryptographic Techniques. - Springer, Berlin, Heidelberg. - 2005. – С. 457-473.

References

1. Proekt GOST Jelektronnaja medicinskaja karta. Terminy i opredelenija. Available at: http://portal.egisz.rosminzdrav.ru/materials/310 (accessed 1 November 2020).

2. S.N. Shcherbo, D.S. Shcherbo. 5P-medicine: precision medicine. Medicine Alphabet. 2015, vol. 18, no. 4, pp. 5 – 10.

3. Zakharov A., Potapov A., Zakharova I., Kotelnikov A., Panfilenko D. (2019, May). Infrastructure of the Electronic Health Record Data Management for Digital Patient Phenotype Creating. In 7th Scientific Conference on Information Technologies for Intelligent Decision-Making Support (ITIDS 2019).Atlantis Press.

4. Joyia G.J., Liaqat R.M., Farooq A., & Rehman S. (2017). Internet of Medical Things (IOMT): applications, benefits and future challenges in healthcare domain. J Commun, 12(4), 240-247.

5. Zakharov A. A., Potapov A. P., Zakharova I. G., Olennikov E. A. (2018, October). Telemetric Medical System to Support Cardiological Screening. In 2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE) (pp. 116-120).

6. Hassan M.K., El Desouky A.I., Elghamrawy S.M., & Sarhan A.M. (2019). A Hybrid Real-time remote monitoring framework with NB-WOA algorithm for patients with chronic diseases. Future Generation Computer Systems, 93, 77-95.

7. Khan, J. Y., Yuce, M. R., Bulger, G., & Harding, B. (2012). Wireless body area network (WBAN) design techniques and performance evaluation. Journal of medical systems, 36(3), 1441-1457.

8. ISO/TR 20514:2005 «Health informatics – Electronic health record – Definition, scope and context». Available at: https://www.iso.org/standard/39525.html (accessed 20 October 2020)

9. Zarubina T.V., Shvyrev S.L.,Solovyev V.G., Rauzina S.E., Radionov V.S., Penzin O.V., Surin M.Y. Integrated electronic health record: Status and Prospects.Vrachiinformacionnyetehnologi. 2016, no. 2.

10. Gehrmann, S., Dernoncourt, F., Li, Y., Carlson, E. T., Wu, J. T., Welt, J., Celi, L. A. (2018). Comparing deep learning and concept extraction based methods for patient phenotyping from clinical narratives. PloS one, 13(2), e0192360.

11. Alexander A. Zakharov, Alexander A. Kotelnikov, Alexander P. Potapov, Dmitry V. Panfilenko, Pavel Y. Gayduk. (2020, October) Information and Analytical Support for Biomedical Research in the Field of the Cardiovascular Disease Risk Prediction. In 8th Scientific Conference on Information Technologies for Intelligent Decision-Making Support (ITIDS 2020). Atlantis Press.

12. Masood, I., Wang, Y., Daud, A., Aljohani, N. R., &Dawood, H. (2018). Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure. Wireless Communications and Mobile Computing, 2018.

13. Kołodziej, J., Grzonka, D., Widłak, A., &Kisielewicz, P. (2019). Ultra Wide Band Body Area Networks: Design and Integration with Computational Clouds. In High-Performance Modelling and Simulation for Big Data Applications (pp. 279-306). Springer, Cham.

14. Edemacu, K., Park, H. K., Jang, B., & Kim, J. W. (2019). Privacy Provision in Collaborative Ehealth With Attribute-Based Encryption: Survey, Challenges and Future Directions. IEEE Access, 7, 89614-89636.

15. Li, M., Yu, S., Ren, K., & Lou, W. (2010, September). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In International conference on security and privacy in communication systems (pp. 89-106). Springer, Berlin, Heidelberg.

16. Sundaravadivel, P., Kougianos, E., Mohanty, S. P., &Ganapathiraju, M. K. (2017). Everything you wanted to know about smart health care: Evaluating the different technologies and components of the Internet of Things for better health. IEEE Consumer Electronics Magazine, 7(1), 18-28.

17. Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., &Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems, 78, 659-676.

18. Lebedev G.S., Shaderkin I.A., Fomina I.V., Lisnenko A.A., Ryabkov I.V., Kachkovsky S.V., Melaev D.V. Internet of medical things: first steps in systematization. Zhurnal telemediciny i jelektronnogo zdravoohranenija. 2017, no. 3(5).

19. MinaevA.A., KuperD.V., Ivaschenko A.V. Moderntrendsindistributed medical diagnostics automation based on the Internet-of-things. Izvestija Samarskogo nauchnogo centra Rossijskoj akademiinauk. 2016, no. 4-4.

20. Bukharev DA, Vagin SV, Sokolov AN Protection of devices of the Internet of things from mirai-like virus worm programs // Journal of the Ural Federal District Information security. - 2018. - No. 4. - S. 11-19.

21. MASLOVA MA Security principles of the Internet of things // Journal of the Ural Federal District Information security Information security. - 2018. - No. 3 (29). - S. 38-42.

22. Wang, C., Liu, X., & Li, W. (2012, September). Implementing a personal health record cloud platform using ciphertext-policy attribute-based encryption. In 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems (pp. 8-14). IEEE.

23. Shamir, A. (1984, August). Identity-based cryptosystems and signature schemes. In Workshop on the theory and application of cryptographic techniques (pp. 47-53). Springer, Berlin, Heidelberg.

24. Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In Annual international cryptology conference (pp. 213-229). Springer, Berlin, Heidelberg.

25. Sahai, A., & Waters, B. (2005, May). Fuzzy identity-based encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 457-473). Springer, Berlin, Heidelberg.

ЗАХАРОВ Александр Анатольевич, доктор технических наук, профессор, заведующий базовой кафедрой «Безопасные информационные технологии Умного города», Институт математики и компьютерных наук, Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: azaharov@utmn.ru

ПОНОМАРЁВ Кирилл Юрьевич, старший преподаватель кафедры информационной безопасности, Институт математики и компьютерных наук, Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: drmckay-kirill@yandex.ru

ZAHAROV Aleksandr, D. Sc. (Tech.), Professor, Head of the Smart City's Secure Information Technologies Department, Institute of Mathematics & Computer Science, Tyumen State University. 625003, Tyumen, Volodarskogo, 6. E-mail: azaharov@utmn.ru

PONOMAREV Kirill, Senior Lecturer of Information Security Department, Institute of Mathematics & Computer Science, Tyumen State University. 625003, Tyumen, Volodarskogo, 6. E-mail: drmckay-kirill@yandex.ru

УДК 004.056.23 Вестник УрФО № 4(38) / 2020, с. 55–63

Ручай А.Н.

DOI: 10.14529/secur200405

РАЗРАБОТКА НОВОГО ПОДХОДА РЕГРЕССИОННОГО ТЕСТИРОВАНИЯ С ПОЛУАВТОМАТИЧЕСКИМ ВЫБОРОМ ТЕСТОВ ДЛЯ АУДИТА IMS БАЗЫ ДАННЫХ

Данная работа посвящена разработке нового подхода регрессионного тестирования с полуавтоматическим выбором тестов. В отличие от предыдущих работ, предложенный подход основывается на полуавтоматическом выборе тестов с учетом различных важных факторов, таких как время выполнения, необходимое количество выполнений тестов, ручной приоритет тестов, результат предыдущих тестов, функциональные возможности тестов. Это позволяет более детально настроить последовательность регрессионных тестов в полуавтоматическом режиме.

Ключевые слова: *тестирование программного обеспечения, регрессионное тестирование, отладка, тестирование на основе ключевых слов, тестирование на основе данных, база данных IMS, выбор тестов.*

Ruchay A.N.

DEVELOPMENT OF A NEW REGRESSION TESTING APPROACH WITH SEMI-AUTOMATIC TEST SELECTION FOR AUDITING AN IMS DATABASE

This work is devoted to the development of a new regression testing approach with semi-automatic test selection. Unlike previous works, the proposed approach is based on semi-automatic selection of tests taking into account various important factors, such as execution time, the required number of test executions, manual priority of tests, the result of previous tests, and test functionality. This allows you to fine-tune the sequence of regression tests in semi-automatic mode.

Keywords: *software testing, regression testing, debugging, keyword driven testing, data driven testing, IMS database, test selection.*

1. Введение

Современные программные проекты развиваются быстро, поскольку разработчики добавляют новые функции, исправляют ошибки или проводят рефакторинг [1, 2, 3]. Чтобы гарантировать, что развитие проекта не нарушит существующую функциональность, разработчики обычно проводят регрессионное тестирование. Однако частый повторный запуск наборов полных регрессионных тестов может занять очень много времени. Для запуска некоторых наборов тестов требуются недели, но ожидание результатов тестирования даже в течение нескольких минут может нанести ущерб рабочему процессу разработки. Помимо снижения производительности, медленное регрессионное тестирование может потреблять много вычислительных ресурсов. В результате большое количество исследований было посвящено снижению затрат на регрессионное тестирование с использованием таких подходов, как выбор регрессионных тестов [4, 5], сокращение набора регрессионных тестов [6, 7], приоритезация регрессионных тестов [8, 9] и распараллеливание тестов.

Подход к регрессионному тестированию, который представлен в данной работе, отличается от других подходов тем, что он использует полуавтоматический процесс выбора тестов для определения приоритетности их выполнения. Приоритизация основана на различных критериях, таких как время выполнения, необходимое количество запусков тестов, ручной приоритет тестов, результат предыдущих тестов, функциональность тестов. Этот подход позволяет более детально настроить последовательность регрессионных тестов.

Работа организована следующим образом. В разделе 2 представлена информация о регрессионном тестировании системы аудита баз данных IMS. В разделе 3 описываются различные подходы к автоматизированному тестированию и автоматизации тестирования. Также в разделе 3 описана структура фреймворка с веб-интерфейсом. Раздел 4 посвящен изучению подхода к выбору регрессионного теста, который ускоряет регрессионное тестирование, а также представлен подход регрессионного тестирования с полуавтоматическим выбором тестов. Наконец, в разделе 5 представлены выводы.

2. Регрессионное тестирование системы аудита IMS базы данных

IBM Information Management System (IMS) – это объединенная иерархическая база данных и система управления информацией с обширными возможностями обработки транзакций [11, 12, 13].

Иерархические базы данных IMS имеют множество преимуществ: это проверенная технология, применяемая в течение многих лет; иерархия (древовидная структура) IMS баз данных проста в использовании. Базы данных IMS способны управлять более 15 миллионами гигабайт данными, обрабатывать транзакции от более 200 миллионов пользователей, и поддерживать более 22000 транзакций в секунду. Основным недостатком иерархических баз данных IMS является их сложность, как с точки зрения правил, так и с точки зрения отношений данных «многие ко многим». Эта сложность привела к тому, что работа с IMS оставалась очень медленной и громоздкой [11, 12, 13].

Система аудита для базы данных IMS на z/OS – это инструмент аудита, который собирает и сопоставляет информацию о доступе к данным из онлайн-регионов IMS, пакетных заданий IMS, наборов данных архивных журналов IMS и записей SMF для получения всестороннего обзора происходящей бизнес-активности в одной или нескольких средах IMS. z/OS – это операционная система для мэйнфреймов IBM, производимая IBM. Система аудита для базы данных IMS помогает аудиторам определить, кто читал или обновлял конкретную базу данных IMS и связанные с ней наборы данных, какой механизм использовался для выполнения этого действия и когда был произведен доступ.

Система аудита для базы данных IMS обеспечивает комплексное решение для аудита, которое снижает затраты на соблюдение нормативных требований за счет автоматизации, централизации и разделения обязанностей. Автоматизация упрощает сбор данных аудита, сокращает ручные усилия, увеличивает производительность, обеспечивает более тщательный аудит и снижает его стоимость. Система аудита для базы данных IMS централизует и сопоставляет информацию из многих систем и источников данных, чтобы обеспечить согласованное представление дан-

ных аудита IMS, создавать отчеты с графическим интерфейсом и пакетные отчеты для проверки данных, а также поддерживать внутренних и внешних аудиторов. Разделение обязанностей обеспечивает целостность данных аудита, устраняет возможность подделки данных, обеспечивает возможность аудиторов не зависеть от разработчиков или администраторов баз данных в настройке или сборе требуемой информации аудита.

Для тестирования системы аудита для баз данных IMS было использовано 50 онлайн-заданий z/OS и 50 пакетных заданий z/OS с 1000 транзакциями в секунду, 10 скриптов стресс-тестирования со 100000 транзакциями в секунду, 1000 транзакций IMS LOG и 3000 SMF транзакций. Наши наборы тестов включали 120 автоматических тестов, 350 тестовых случаев, 4 версии системы аудита для базы данных IMS, 4 версии баз данных IMS и 3 подсистемы z/OS.

Постоянное регрессионное тестирование (общее тестирование, тестирование безопасности, тестирование производительности, стресс-тестирование) необходимо, чтобы гарантировать, что добавление новых функций, исправлений или рефакторингов не нарушит существующую функциональность. Однако частый повторный запуск наборов полных регрессионных тестов требует очень много времени. Для выполнения этого тестирования могут потребоваться недели и это может нанести ущерб рабочему процессу разработки. Помимо снижения производительности труда разработчиков, медленное регрессионное тестирование может потреблять значительные вычислительные ресурсы. Нашему регрессионному тестированию требуется около 3 месяцев для запуска всех тестов вручную. Основная цель заключалась в создании среды автоматизации тестирования, которая сокращает время регрессионного тестирования.

3. Избирательная мультибиометрическая аутентификация

Автоматическое тестирование – это выполнение тестовых примеров в автоматическом режиме без ручного вмешательства [14]. Автоматизация тестирования включает в себя различные действия, такие как создание тестов, создание отчетов о результатах выполнения тестов и управление тестированием. Этот метод тестирования эволюционировал в течение пяти поколений [15, 16]: запись и воспроизведение, пользовательские скрипты, тестирование на основе данных, тестирование на основе ключевых слов, и тестирование, управляемое процессами.

Фреймворк автоматизации тестирования – это интегрированная система, которая устанавливает правила, по которым продукт проходит автоматическое тестирование. Среда автоматизации тестирования объединяет библиотеки функций, источники тестовых данных, сведения об объектах и различные повторно используемые модули. Фреймворк обеспечивает основу для тестирования и упрощает автоматизацию. Наиболее распространенные подходы автоматизации тестирования являются [15, 16]: тестирование на основе модулей; тестирование под управлением данными; тестирования под управлением ключевыми словами; и гибридное тестирование.

Тестирование на основе модулей – это базовый подход автоматизации тестирования. Платформа тестирования на основе модулей использует сценарии тестирования, которые соответствуют функциональности продукта и соответствуют конкретным модулям приложения. Эти тестовые сценарии используются иерархически для создания больших тестовых примеров. Структура тестирования на основе модулей назначает независимые тестовые сценарии конкретным программным компонентам, модулям или функциям.

В подходе автоматизации тестирования под управлением данными тестовые данные отделяются от тестовых сценариев, и результаты тестирования сравниваются с тестовыми данными. Когда тесты используют различные наборы входных и выходных тестовых данных, среды тестирования на основе данных более эффективны и проще в управлении.

В подходе автоматизации тестирования под управлением ключевыми словами ключевые слова написаны таким образом, чтобы они соответствовали функциональности на уровне модулей. Фреймворк тестирования на основе ключевых слов не зависит от приложения и использует методы таблицы данных и ключевые слова для выполнения действий.

Гибридное тестирование включают в себя модульные сценарии, фреймворк на основе данных и функциональная декомпозиция. Платформа гибридного тестирования может быть более сложной для первоначальной настройки, чем другие платформы. Одна-

ко инфраструктуры гибридного тестирования могут обеспечить максимальную гибкость, если они будут тщательно оценены и внедрены.

Используемая нами структура автоматизации тестирования состоит из системы проектирования тестов, системы мониторинга тестирования и системы выполнения тестов [17].

Веб-интерфейс, который мы использовали с нашей платформой автоматизации тестирования, был разработан с помощью Qooxdoo, среды веб-приложений Ajax с открытым исходным кодом. Это клиентское, независимое от сервера решение, которое включает поддержку профессиональной разработки на JavaScript [18], набор инструментов графического пользовательского интерфейса (GUI) и высокоуровневую связь между клиентом и сервером.

Библиотеки Java, которые мы использовали для разработки нашей среды автоматизации тестирования, включают: S3270 для интеграции системы TN3270 на z/OS, Selenium WebDriver для экземпляра браузера, Ganymed SSH-2 для реализации протокола SSH-2, Apache Commons Net для реализации на стороне клиента основных интернет-протоколов, Apache FreeMarker для генерации текстового вывода на основе шаблонов и изменения данных, Jsoup для работы с реальным HTML, Gson для сериализации и десериализации Java-объектов в JSON, Apache log4j для ведения журнала, httpclient для реализации клиентской части.

Система дизайна тестов используется для создания новых тестов и редактирования существующих. Её легко использовать при минимальном обучении и без навыков программирования. Созданные тестовые данные можно хранить в файлах. Простым решением является использование существующего инструмента, такого как редактор JSON, в качестве системы проектирования тестов [19]. JSON – это формат открытого стандарта, в котором для передачи объектов данных, состоящих из пар атрибут-значение, который способен воспринять человек. Это наиболее распространенный независимый от языка формат данных, используемый для асинхронной связи между браузером и сервером. JSON предлагает ряд преимуществ по сравнению с XML: его можно быстрее анализировать, он более компактен, с ним легче работать на некоторых языках и при форматировании его, как правило, легче читать.

Система контроля тестирования используется для контроля выполнения теста и проверки результатов тестирования. Она имеет следующие возможности: запуск выполнения теста вручную; запускать выполнение теста автоматически после определенного события; автоматический запуск выполнения теста в указанное время; остановка выполнения теста; мониторинг выполнения теста во время выполнения тестов; просмотр журналов тестирования во время выполнения тестов и после них; просмотр отчета тестирования; изменение уровня ведения журнала; выбор регрессионных тестов; настройка тестов. Решение для мониторинга тестирования использует веб-интерфейс для запуска и остановки выполнения теста, а также для создания журналов и отчетов в формате HTML и JSON.

Система выполнения тестов это ядро фреймворка. Его основными компонентами являются скрипты драйверов, тестовая библиотека, анализатор тестовых данных и другие утилиты, такие как генератор журналов и отчетов. Выполнение теста контролируется скриптами драйвера, которые запускаются с помощью системы мониторинга тестирования. Скрипты драйверов имеют несложную структуру, поскольку они в основном используют службы, предоставляемые тестовыми библиотеками и другими повторно используемыми модулями. Библиотеки тестирования содержат функции и модули, которые используются при тестировании или в поддерживающих его действиях. Тестирование – это в основном взаимодействие с тестируемой системой и проверка ее правильности. Функции в тестовой библиотеке могут выполнять свои задачи независимо, но они также могут использовать другие функции или даже внешние инструменты. Например, фреймворк TN3270 используется для реализации работы с z/OS и базой данных IMS, framework Selenium [20] и REST API – веб-интерфейс системы аудита для базы данных IMS. Анализатор тестовых данных предназначен для простого предоставления тестовых данных сценариям драйвера с помощью анализатора JSON в Java. Его задача – обработать тестовые данные и вернуть их скрипту драйвера в простых в использовании контейнерах тестовых данных.

Используемая в нашем исследовании среда автоматизации тестирования была построена с использованием нескольких по-

вторно используемых модулей и библиотек функций, которые имеют следующие особенности:

• Удобство обслуживания: фреймворк значительно снижает затраты на обслуживание.

• Возможность повторного использования: тестовые примеры и функции библиотеки можно использовать повторно.

• Управляемость: эффективный дизайн тестов, отслеживаемость и выполнение.

• Удобство разработки: легко разрабатывать, проектировать, изменять и отлаживать тесты во время выполнения.

• Доступность: позволяет запланировать выполнение автоматизации.

• Надежность: расширенная обработка ошибок и восстановление сценариев.

• Гибкость: структура, независимая от тестируемой системы.

• Измеримость: настраиваемая отчетность о результатах тестирования обеспечивает качественный результат.

Требования высокого уровня к крупномасштабным средам автоматизации тестирования – автоматическое выполнение тестов, простота использования и ремонтопригодность. Наша структура удовлетворяет следующим требованиям [16, 15]:

Требования высокого уровня. Фреймворк автоматически выполняет тесты, прост в использовании без навыков программирования, прост в поддержке, не требует постоянного контроля при выполнении тестов. Это позволяет запускать тесты вручную или планировать автоматическое выполнение в заранее определенное время или после определенных событий. Нефатальные ошибки, вызванные тестовой средой, обрабатываются и сообщаются без остановки выполнения теста. Результаты тестов адекватны и могут быть в ручную перепроверены. Каждый выполненный тест помечается как пройденный или неудачный, а неудачные тесты имеют короткое сообщение об ошибке. Выполнение теста регистрируется с использованием различных настраиваемых уровней ведения журнала. Отчет тестирования создается и публикуется автоматически.

Простота использования. Фреймворк использует подход, основанный на ключевых словах, поддерживает создание пользовательских ключевых слов. Он предоставляет функциональные возможности, которые выбирают и группируют тесты для конкретной задачи.

Удобство обслуживания. Фреймворк является модульным и имеет соглашения о кодировании и именовании. Он реализован с использованием языков сценариев высокого уровня. Тестовое ПО в структуре находится под контролем версий (Git) и должным образом документировано.

Для регрессионного тестирования разработанная автоматизация тестирования требует 3 недели вместо 3 месяцев ручного тестирования.

4. Предлагаемое регрессионное тестирование с полуавтоматическим выбором тестов

Широко используемый метод ускорения регрессионного тестирования называется отбором регрессионного теста (RTS) [1]. RTS сокращает время тестирования за счет повторного запуска только тех тестов, на которые повлияло изменение кода. RTS – надежный метод, если он проверяет все сценарии, на которые может повлиять изменение кода. Если какие-либо сценарии, на которые повлияло изменение кода, не тестируются, регрессией могут быть пропущены. Существующие подходы RTS можно разделить на динамические и статические методы.

Отсутствие практичных инструментов RTS оставляет разработчикам два варианта: они должны либо автоматически перезапустить все тесты, либо выполнить ручной выбор тестов (ручной RTS). Автоматический повторный запуск всех тестов – безопасный подход, но он может быть неточным и неэффективным. Напротив, ручной RTS может быть небезопасным и неточным по нескольким причинам. При использовании RTS вручную разработчики могут выбрать слишком мало тестов и, как следствие, исключить тесты, которые могут выявить различия из-за изменений кода. Они также могут выбрать слишком много тестов и, таким образом, безрезультатно потратить время. Таким образом, разработчики могут извлечь выгоду из автоматизированного метода RTS, который чаще всего работает на практике. Не установлено, насколько ручные методы RTS, используемые разработчиками, сравниваются с автоматизированными методами RTS, предлагаемыми в литературе.

Существует следующие методы выбора регрессионного теста [21]:

• Метод повторного тестирования: этот метод тестирует все тесты, которые ранее выполнялись. Данный метод очень дорогостоя-

щий, так как наборы регрессионных тестов достаточно большие.

• Техника случайного/специального назначения. При использовании этой техники тестировщики полагаются на свой предыдущий опыт и знания, чтобы выбрать, какие тесты необходимо повторить. Это может включать случайный выбор процента покрытия тестов.

• Метод потока данных. Этот метод представляет собой метод выбора регрессионного теста на основе покрытия только тех тестов, которые проверяют взаимодействие данных, имеющих влияние из-за изменений кода.

• Безопасный метод. Этот метод исключает тесты, которые вряд ли обнаружат ошибки. Этот метод обычно выбирает почти все тесты, когда в коде были внесены существенные изменения. Этот метод не фокусируется на критериях покрытия, а выбирает все тесты, которые проверяют результат работы измененной программы по сравнению с ее исходной версией.

• Гибридный метод. Этот метод включает в себя приоритизацию тестовых примеров и минимизацию регрессионных тестов.

В отличие от предыдущих работ [8], мы предлагаем комбинированный подход к выбору последовательности тестов, который использует простые критерии и правила, такие как общие усилия, время выполнения, время развертывания и т.д. Для этого требуются ручные и автоматические настройки.

Основные критерии и правила выбора полуавтоматического регрессионного теста с точки зрения нашего подхода включают:

1. Суммарные усилия, количество необходимых тестов.

2. Требуемое время для тестов, общее время выполнения.

3. Требуемое количество конкретных тестов.

4. Наличие необходимых баз данных IMS, подсистем z/OS.

5. Приоритет тестов.

6. Результаты предыдущих тестов.

Предлагаемое нами регрессионное тестирование с полуавтоматическим выбором тестов отдает приоритет тестам на основе наивысшего приоритета в соответствии с вышеуказанными основными критериями и правилами.

Рассмотрим набор тестов *T*, содержащий *n* тестов, $\{t_1, t_2, \dots, t_n\}$. Для теста t_i определим набор атрибутов $a_i \subseteq A$. Представим как набор функций аудита базы данных IMS, задаваемый вручную тестером. Функциональные возможности аудита базы данных IMS определяются 10 типами фильтрации и 7 типами информации для аудита базы данных IMS.

Для любого t_i теста пусть

$$p_i = \prod_{j=1}^{k} t_i^j$$

обозначает приоритет использования теста, где t_i^j - оценка фактора использования теста на основе j критерия.

Были использованы следующие критерии j для t_i теста в предлагаемом регрессионном тестировании с полуавтоматическим выбором тестов:

• $t^1 = \{0,1\}$ - коэффициент наличия необходимой подсистемы z/OS, версия системы аудита для базы данных IMS, версия базы данных IMS. если доступен и если недоступен.

• $t^2 = [1,10]$ - приоритет теста. Тестер устанавливает этот коэффициент для каждого теста t_i. Например, для высокого приоритета $t^2 = 10$.

• $t^3 = [1, d]$ - коэффициент результата предыдущих тестов. Этот коэффициент рассчитывается для всех предыдущих тестов. d - количество программных сбоев, выявленных тестом t_i.

• $t^4 = [1,20]$ - необходимое количество запусков теста. Тестер устанавливает этот коэффициент для каждого t_i теста. Например, для работ с высоким риском отказа $t^4 = 10$.

• $t^5 = [0,10]$ - коэффициент требований спецификации на основе информации от разработчиков.

• $t^6 = [1,10]$ - коэффициент времени выполнения тестов. Например, для длинного теста $t^6 = 1$ и короткого теста $t^6 = 10$.

Нами был предложен следующий алгоритм, который определяет приоритетность использования тестов для регрессионного тестирования с полуавтоматическим выбором тестов:

1. Определить подсистему z/OS, версию системы аудита для базы данных IMS на z/OS, версию баз данных IMS.

2. Определить критерии t_i, некоторые из них нужно указать вручную.

3. Определить *T'* подмножество тестов в соответствии с подмножеством *A*.

4. Оцените приоритет $\{p_1, \dots, p_n\}$ использования тестов, оценив все критерии.

5. Упорядочить t_i тесты в подмножестве T' согласно значениям p_i.

Для регрессионного тестирования на основе предложенного подхода требуется один день для дымового тестирования и одна неделя для подробного регрессионного тестирования, чтобы удовлетворить требованиям разработчиков и клиентов. Вместо того, чтобы сосредоточиться только на сокращении количества выбранных тестов, наш подход обеспечивает значительное сокращение времени регрессионного тестирования и уравновешивает время, необходимое для анализа, сбора и выполнения тестов.

5. Заключение

Регрессионное тестирование важно для проверки того, что изменения программного обеспечения не нарушают ранее работающую функциональность. Однако регрессионное тестирование обходится дорого, потому, что оно запускает множество тестов для многих версий. Хотя RTS, предложенная более трех десятилетий назад, обеспечивает многообещающий подход к ускорению регрессионного тестирования, ни один метод RTS не получил широкого распространения на практике из-за проблем с эффективностью и безопасностью.

Большинство разработчиков выполняют RTS вручную. Они выбирают тесты специальными способами, которые потенциально не выявляют ошибок или теряя время [4]. Представленный здесь подход предлагает регрессионное тестирование с полуавтоматическим выбором тестов. Этот подход определяет приоритеты тестов на основе приоритета в соответствии с некоторым критерием.

Подход к регрессионному тестированию, который мы представляем здесь, отличается от других подходов тем, что он использует полуавтоматический процесс выбора тестов для определения приоритетности их выполнения. Приоритизация основана на различных критериях, таких как время выполнения, необходимое количество запусков тестов, ручной приоритет тестов, результат предыдущих тестов, функциональность тестов. Этот подход позволяет более детально настроить последовательность регрессионных тестов вручную.

Представленный в данной работе подход обеспечивает существенное сокращение времени, необходимого для регрессионного тестирования, и уравновешивает время, необходимое для анализа, сбора и выполнения, вместо того, чтобы сосредоточиться исключительно на сокращении количества выбранных тестов.

В данном исследовании оценивалась осуществимость представленной среды автоматизации тестирования для регрессионного тестирования системы аудита баз данных IMS. Общая оценка была положительной, и фреймворк был признан эффективным. Представленная структура автоматизации тестирования удовлетворяет важным требованиям более низкого уровня с точки зрения простоты использования и удобство обслуживания.

Литература

1. Legunsen O., Hariri F., Shi A., Lu Y., Zhang L., Marinov D. An extensive study of static regression test selection in modern software evolution. Proceedings of the 2016 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering, 2016, pp. 583–594.

2. Tulpule N. Strategies for testing client-server interactions in mobile applications: How to move fast and not break things. Proceedings of the 2013 ACM Workshop on Mobile Development Lifecycle, 2013, pp. 19–20.

3. Jensen C. S., Moller A., Su Z. Server interface descriptions for automated testing of javascript web applications. Proceedings of the 2013 9th Joint Meeting on Foundations of Software Engineering, 2013, pp. 510–520.

4. Gligoric M., Eloussi L., Marinov D. Practical regression test selection with dynamic file dependencies. Proceedings of the 2015 International Symposium on Software Testing and Analysis, 2015, pp. 211–222.

5. Rothermel G., Harrold M. J. A safe, efficient regression test selection technique. ACM Trans. Softw. Eng. Methodol., 1997, vol. 6, no. 2, pp. 173–210.

6. Shi A., Yung T., Gyori A., Marinov D. Comparing and combining test-suite reduction and regression test selection. Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering, 2015, pp. 237–247.

7. Zhong H., Zhang L., Mei H. An experimental study of four typical test suite reduction techniques. Information and Software Technology, 2008, vol. 50, no. 6, pp. 534–546.

8. Hao D., Zhang L., Zhang L., Rothermel G., Mei H. A unified test case prioritization approach. ACM Trans. Softw. Eng. Methodol., 2014, vol. 24, no. 2, pp. 10:1–31.

9. Zhai K., Jiang B., Chan W. K. Prioritizing test cases for regression testing of location-based services: Metrics, techniques, and case study. IEEE Trans. Serv. Comput., 2014, vol. 7, no. 1, pp. 54–67.

10. Yoo S., Harman M. Regression testing minimization, selection and prioritization: A survey. Softw. Test. Verif. Reliab., 2012, vol. 22, no. 2, pp. 67–120.

11. Klein B., Long R. A., Blackman K. R., Goff D. L., Nathan S. P., Lanyi M. M., Wilson M. M., Butterweck J., Sherrill S. L. An Introduction to IMS: Your Complete Guide to IBM Information Management System. IBM Press, 2nd ed., 2012.

12. Burleson D. K. Inside the Database Object Model. Boca Raton, FL, USA: CRC Press, Inc., 1st ed., 1998.

13. Long R., Harrington M., Hain R., Nicholls G. IMS Primer. USA: IBM Redbook, 2000.

14. Bajpai R. N. A Keyword Driven Framework for Testing Web Applications. International Journal of Advanced Computer Science and Applications (IJACSA), 2012, vol. 3, no. 3.

15. Abhishek K., Kumar P., Sharad T. Automation of Regression Analysis: Methodology and Approach, 2012, pp. 481–487.

16. Kumar P., Kavita D. Automation framework for database testing. 5th International Conference on Recent Innovations in Science, Engineering and Management, 2016, pp. 88–93.

17. Laukkanen P. Data-driven and keyword-driven test automation frameworks, 2007.

18. Artzi S., Dolby J., Jensen S. H., Moller A., Tip F. A framework for automated testing of javascript web applications. Proceedings of the 33rd International Conference on Software Engineering, 2011, pp. 571–580.

19. Sabev P., Grigorova K. Manual to automated testing: An effort-based approach for determining the priority of software test automation. International Journal of Computer, Electrical, Automation, Control and Information Engineering, 2015, vol. 9, no. 12, pp. 2456–2462.

20. Gojare S., Joshi R., Gaigaware D. Analysis and design of selenium webdriver automation testing framework. Procedia Computer Science, 2015, vol. 50, pp. 341–346.

21. Jyoti K. S. A comparative study of five regression testing techniques: A survey. International journal of scientific & technology research, 2014, vol. 3, pp. 76–80.

22. Ruchay A.N. A regression testing with semi-automatic test selection for auditing of ims database // Chelyabinsk Physical and Mathematical Journal, 4(2), 2019. Pp. 241-249.

23. Агафонов А.В., Синадский Н.И. Тестирование защищенности телекоммуникационного оборудования от сетевых компьютерных атак типа «отказ в обслуживании» с применением генетического алгоритма // Вестник УрФО. Безопасность в информационной сфере № 2(24), 2017. С. 4-8.

References

1. Legunsen O., Hariri F., Shi A., Lu Y., Zhang L., Marinov D. An extensive study of static regression test selection in modern software evolution. Proceedings of the 2016 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering, 2016, pp. 583–594.

2. Tulpule N. Strategies for testing client-server interactions in mobile applications: How to move fast and not break things. Proceedings of the 2013 ACM Workshop on Mobile Development Lifecycle, 2013, pp. 19–20.

3. Jensen C. S., Moller A., Su Z. Server interface descriptions for automated testing of javascript web applications. Proceedings of the 2013 9th Joint Meeting on Foundations of Software Engineering, 2013, pp. 510–520.

4. Gligoric M., Eloussi L., Marinov D. Practical regression test selection with dynamic file dependencies. Proceedings of the 2015 International Symposium on Software Testing and Analysis, 2015, pp. 211–222.

5. Rothermel G., Harrold M. J. A safe, efficient regression test selection technique. ACM Trans. Softw. Eng. Methodol., 1997, vol. 6, no. 2, pp. 173–210.

6. Shi A., Yung T., Gyori A., Marinov D. Comparing and combining test-suite reduction and regression test selection. Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering, 2015, pp. 237–247.

7. Zhong H., Zhang L., Mei H. An experimental study of four typical test suite reduction techniques. Information and Software Technology, 2008, vol. 50, no. 6, pp. 534–546.

8. Hao D., Zhang L., Zhang L., Rothermel G., Mei H. A unified test case prioritization approach. ACM Trans. Softw. Eng. Methodol., 2014, vol. 24, no. 2, pp. 10:1–31.

9. Zhai K., Jiang B., Chan W. K. Prioritizing test cases for regression testing of location-based services: Metrics, techniques, and case study. IEEE Trans. Serv. Comput., 2014, vol. 7, no. 1, pp. 54–67.

10. Yoo S., Harman M. Regression testing minimization, selection and prioritization: A survey. Softw. Test. Verif. Reliab., 2012, vol. 22, no. 2, pp. 67–120.

11. Klein B., Long R. A., Blackman K. R., Goff D. L., Nathan S. P., Lanyi M. M., Wilson M. M., Butterweck J., Sherrill S. L. An Introduction to IMS: Your Complete Guide to IBM Information Management System. IBM Press, 2nd ed., 2012.

12. Burleson D. K. Inside the Database Object Model. Boca Raton, FL, USA: CRC Press, Inc., 1st ed., 1998.

13. Long R., Harrington M., Hain R., Nicholls G. IMS Primer. USA: IBM Redbook, 2000.

14. Bajpai R. N. A Keyword Driven Framework for Testing Web Applications. International Journal of Advanced Computer Science and Applications (IJACSA), 2012, vol. 3, no. 3.

15. Abhishek K., Kumar P., Sharad T. Automation of Regression Analysis: Methodology and Approach, 2012, pp. 481–487.

16. Kumar P., Kavita D. Automation framework for database testing. 5th International Conference on Recent Innovations in Science, Engineering and Management, 2016, pp. 88–93.

17. Laukkanen P. Data-driven and keyword-driven test automation frameworks, 2007.

18. Artzi S., Dolby J., Jensen S. H., Moller A., Tip F. A framework for automated testing of javascript web applications. Proceedings of the 33rd International Conference on Software Engineering, 2011, pp. 571–580.

19. Sabev P., Grigorova K. Manual to automated testing: An effort-based approach for determining the priority of software test automation. International Journal of Computer, Electrical, Automation, Control and Information Engineering, 2015, vol. 9, no. 12, pp. 2456–2462.

20. Gojare S., Joshi R., Gaigaware D. Analysis and design of selenium webdriver automation testing framework. Procedia Computer Science, 2015, vol. 50, pp. 341–346.

21. Jyoti K. S. A comparative study of five regression testing techniques: A survey. International journal of scientific & technology research, 2014, vol. 3, pp. 76–80.

22. Ruchay A.N. A regression testing with semi-automatic test selection for auditing of ims database // Chelyabinsk Physical and Mathematical Journal, 4(2), 2019. Pp. 241-249.

23. Agafonov A.V.. Sinadskiy N.I. Testirovaniye zashchishchennosti telekommunikatsionnogo oborudovaniya ot setevykh kompyuternykh atak tipa «otkaz v obsluzhivanii» s primeneniyem geneticheskogo algoritma // Vestnik UrFO. Bezopasnost v informatsionnoy sfere № 2(24). 2017. C. 4-8.

РУЧАЙ Алексей Николаевич, кандидат физико-математических наук, доцент, заведующий кафедрой компьютерной безопасности и прикладной алгебры, Челябинский государственный университет. 454001, Россия, г. Челябинск, ул. Братьев Кашириных, 129; доцент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, Россия, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: ran@csu.ru

RUCHAY Alexey, PhD in Physics and Mathematics, Associate Professor, Head of the Department of Computer Security and Applied Algebra, Chelyabinsk State University. 454001, Russia, Chelyabinsk, st. Kashirin Brothers, 129; Associate Professor, Department of Information Security, South Ural State University (National Research University), 454080, Russia, Chelyabinsk, etc. them. IN AND. Lenin, 76. E-mail: ran@csu.ru

УДК 004.896 + 004.056.5 Вестник УрФО № 4(38) / 2020, с. 64–68

Алабугин С.К., Соколов А.Н.

DOI: 10.14529/secur200406

ИСПОЛЬЗОВАНИЕ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ НЕЙРОННЫХ СЕТЕЙ ПРИ ВЫЯВЛЕНИИ АНОМАЛИЙ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

Рассмотрены генеративно-состязательные нейронные сети, а также их применение в задаче выявления аномалий технологического процесса. Для проведения экспериментов использовался набор данных Gas Pipeline, описывающий работу системы бензопровода. В ходе экспериментальных исследований, на примерах, соответствующих нормальному состоянию технологического процесса, была обучена генеративно-состязательная модель BiGAN. Показаны преимущества применения генеративно-состязательных моделей в задаче выявления аномалий технологического процесса.

Ключевые слова: *информационная безопасность, автоматизированные системы управления технологическими процессами, выявление аномалий, глубокое обучение, генеративно-состязательные сети.*

Alabugin S.K., Sokolov A.N.

GENERATIVE ADVERSARIAL NETWORKS USAGE IN DETECTING ANOMALIES OF THE INDUSTRIAL PROCESS

The paper considers generative adversarial networks (GAN) and their application in industrial process anomaly detection. Experiments were conducted using the Gas Pipeline dataset. This dataset describes the operation of the gas pipeline system. In the course of experimental studies, the generative-adversarial model BiGAN was trained only on examples corresponding to the normal state of the industrial process. The advantages of the use of generative adversarial models in the problem of industrial process anomaly detection are shown.

Keywords: *information security, industrial control systems, anomaly detection, deep learning, generative adversarial networks.*

Автоматизированные системы управления технологическим процессом (АСУ ТП) часто размещаются на индустриальных объектах, от работы которых зависит качество жизни значительного числа граждан и/или экономическое благополучие отдельного региона или страны. По этой причине индустриальные объекты и размещенные на них АСУ ТП могут оказаться целью кибератак, приводящих, в том числе, к остановке производства, техногенным катастрофам, материальным и репутационным потерям [1-3].

Поскольку современная АСУ ТП является не только информационной, но и физической системой, один из способов обнаружения вторжений заключается в мониторинге непосредственно технологического процесса и выявление аномалий. Зачастую, аномалия указывает на неправильную работу системы, которая, возможно, вызвана кибератакой.

Среди нескольких имеющихся подходов к выявлению аномалии, основанных на использовании машинного обучения [4] выделяются генеративно–состязательные нейронные сети (Generative adversarial network, GAN) [5]. Генеративно-состязательный нейронные сети представляют собой специфический класс нейронных сетей, в архитектуре которых имеются две модели: генератор и дискриминатор. Архитектура такой сети представлена на рис. 1.

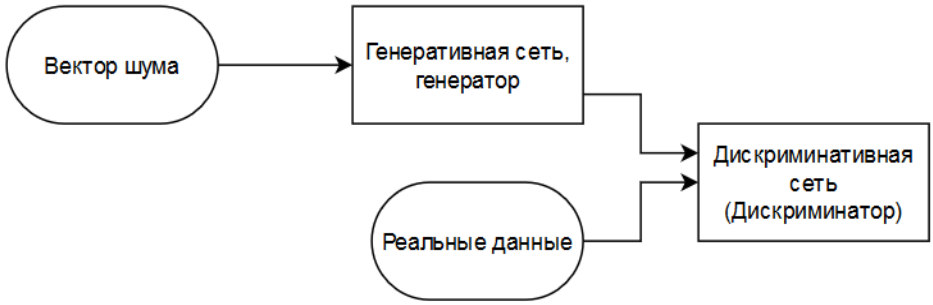


Рис.1 Схема генеративно-состязательной сети

Генератору G на вход подаётся вектор, состоящий из случайного шума – вектор из некоторого пространства скрытых переменных (latent space) Z, на котором задано априорное распределение $p_z(z)$. На выходе генератор выдаёт новый объект из пространства данных X. Формально, сеть-генератор можно описать в виде следующей функции:

$$G=G(z;\theta_g): Z \longrightarrow X$$

где θ_g – параметры сети-генератора. В ходе обучения, генератор аппроксимирует распределение p_{data}, выборки реальных данных X. Следовательно, по окончании обучения, распределение порождаемых генератором объектов p_{gen}, должно быть приближенно к распределению реальных объектов p_{data}.

Для того, чтобы генератор с каждой итерацией обучения обладал лучшей аппроксимацией распределения p_{data}, используется сеть дискриминатор. Дискриминатор – как правило, является обычным бинарным классификатором, на вход которому подаётся объект x из пространства данных X. На выходе, дискриминатор выдаёт вероятность принадлежности объекта к тому или иному классу: реальный объект или объект, порождённый дискриминатором. Формально, дискриминатор определяется как:

$$D=D(x;\theta_d): X \longrightarrow [0,1]$$

где θ_d – параметры сети-дискриминатора. Для того, чтобы аппроксимировать распределение p_{data}, генератору нужно научиться обманывать дискриминатор: научиться порождать такие объекты, которые дискриминатор не в состоянии отличить от настоящих.

В настоящее время генеративно-состязательные сети применяются, в частности, для генерации синтетических изображений [6-7]. В ходе обучения, сеть учится аппроксимировать статистическое распределение, задаваемое реальными данными, или, говоря точнее, генератор учится отображать простое распределение (из которого берутся векторы шума) в сложное, произвольное распределение реальных данных.

Было предложено несколько способов применения GAN в задаче выявления аномалий. Мы рассмотрим один из них, основанный на применении архитектуры Bidirectional Generative Adversarial Network (BiGAN, двунаправленная генеративно-состязательная сеть) [8]. Схема архитектуры BiGAN представлена на рис. 2.

В обычную схему GAN добавлена сеть-кодировщик (encoder, E), которая отображает

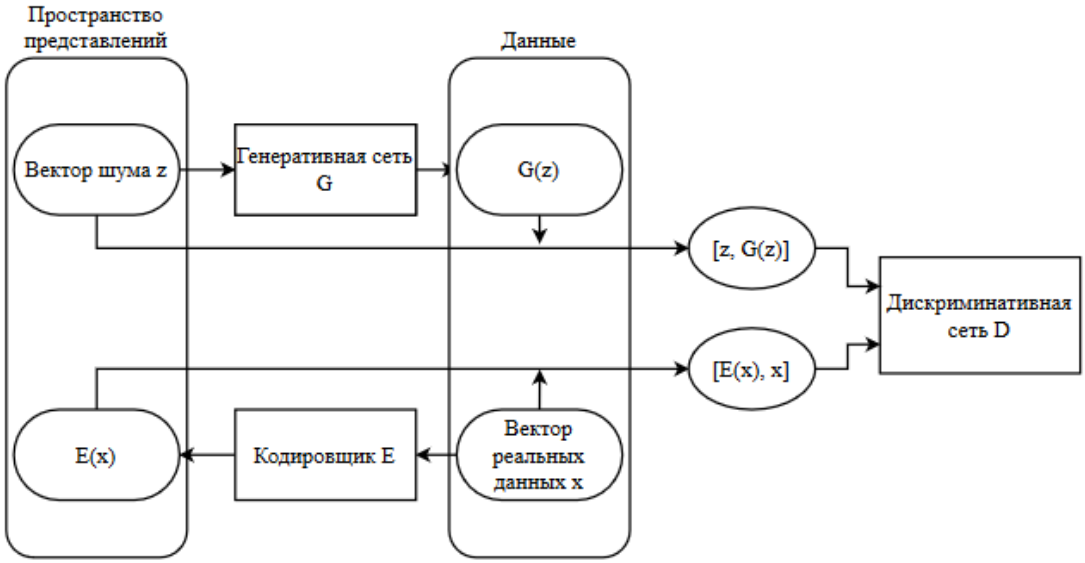


Рис.2 Схема сети BiGAN

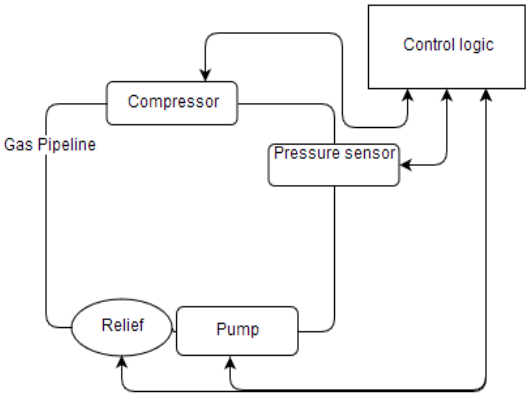


Рис.3 Схема установки Gas Pipeline

ся генератору. Таким образом, выход генератора отображается в пространство реальных данных. После этого мы можем считать метрикой аномальности расстояние до ближайшего примера из реальных данных.

Для проведения экспериментов, в исследовании использовался набор данных Gas Pipeline [9]. В нём представлены данные, соответствующие нормальной работе системы и данные, соответствующие различным атакам. Схема системы представлена на рис. 3.

Система состоит из бензопровода, помпы, компрессора, датчика давления и предохранительного клапана, управляемого соленоидом. Необходимый уровень давления в системе поддерживается с помощью пропорционально-интегрально-дифференцирующего (ПИД) регулятора. Для коммуникации в описанной системе используется протокол прикладного уровня Modbus. Сетевые пакеты с метками времени после некоторой обработки составляют набор данных, таким образом запись набора данных соответствует сетевому пакету Modbus. Каждая запись содержит значения 16 признаков, некоторые из которых несут в себе информацию о сети (адрес назначения пакета, код функции Modbus и т.д.), а остальные - характеризуют состояние технологического процесса.

Экспериментальные исследования были проведены при помощи библиотеки машинного обучения Tensorflow. Для применения BiGAN были реализованы модели генератора, дискриминатора и кодировщика. Каждая из этих моделей является обычной полносвязной сетью.

Так как в наборе данных часто встречаются пропуски (в частности, среди значений признаков, описывающих состояние технологического процесса), а значения разных признаков имеют существенно различающиеся масштабы, данные были подвергнуты предобработке. Для заполнения пропусков использовались последние известные значения признака. После этого, данные были разделены на обучающую и тестовую выборки: в обучающую выборку было включено 95% всех записей, описывающих нормальную работу системы. Все признаки были нормализованы относительно обучающей выборки.

Обучение модели BiGAN осуществлялось в течении 50 эпох, лучшие результаты были получены на 39-й эпохе. Уже обученная модель тестировалась следующим образом: объект из тестовой выборки подавался на

вход кодировщику, а выхлоп кодировщика подавался генератору. В пространстве данных находилось расстояние между полученным объектом и ближайшим настоящим объектом, соответствующим нормальной работе системы. Это расстояние использовалось в качестве метрики аномальности, и, для получения лучших результатов, был подобрано пороговое значение. Лучшие, полученные после подбора порога, результаты, в сравнении с несколькими уже известными представлены в табл. 1.

Как видно из таблицы, полученные на наборе данных Gas Pipeline результаты, не являются лучшими. Однако, в силу своей специфики, используемый подход не требует для обучения примеров, соответствующих вторжению, и обучался лишь на данных, соответствующих нормальной работе системы. На практике, это является очень важным преимуществом, так как позволяет затратить меньшее сил на подготовку обучающего набора данных.

Таблица 1

Результаты экспериментов

Алгоритм	Accuracy	Precision	Recall
Исследуемая модель	0.95	0.93	0.98
Сеть Байеса	0.87	0.97	0.59
Support Vector Data Description	0.76	0.95	0.21
Isolation Forest	0.70	0.51	0.13
K-means	0.57	0.83	0.57
Support Vector Machine (SVM)	0.94	0.94	0.94
Random Forest	0.99	0.99	0.99

Литература

1. Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. Stuxnet Dossier Version 1.4. Symantec Security Response.

2. Lee, R., Assante, M., & Connway, T. (2014). ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper–German steel mill cyber attack. Sans ICS.

3. Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid. SANS Industrial Control Systems, 23.

4. Асяев Г. Д., Соколов А. Н. Обнаружение вторжений на основе анализа аномального поведения локальной сети с использованием алгоритмов машинного обучения с учителем //Вестник УрФО. Безопасность в информационной сфере. – 2020. – №. 1 (35). – С. 77-83.

5. Goodfellow I. et al. Generative adversarial nets //Advances in neural information processing systems. – 2014. – С. 2672-2680

6. Reed S. et al. Generative Adversarial Text to Image Synthesis //International Conference on Machine Learning. – 2016. – С. 1060-1069.

7. Karras T., Laine S., Aila T. A style-based generator architecture for generative adversarial networks // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. – 2019. – С. 4401-4410.

8. Donahue J., Krähenbühl P., Darrell T. Adversarial feature learning //arXiv preprint arXiv:1605.09782. – 2016.

9. Morris T. H., Thornton Z., Turnipseed I. Industrial control system simulation and data logging for intrusion detection system research //7th annual southeastern cyber security summit. – 2015. – С. 3-4.

References

1. Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. Stuxnet Dossier Version 1.4. Symantec Security Response.

2. Lee, R., Assante, M., & Connway, T. (2014). ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper–German steel mill cyber attack. Sans ICS.

3. Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid. SANS Industrial Control Systems, 23.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта № 16/2020.

4. Asyaev G. D., Sokolov A. N. Obnaruzhenie vtorzhenij na osnove analiza anomal'nogo povedenija lokal'noj seti s ispol'zovaniem algoritmov mashinnogo obuchenija s uchitelem //Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2020. – no. 1(35). – pp. 77-83.

5. Goodfellow I. et al. Generative adversarial nets //Advances in neural information processing systems. – 2014. – C. 2672-2680

6. Reed S. et al. Generative Adversarial Text to Image Synthesis //International Conference on Machine Learning. – 2016. – C. 1060-1069.

7. Karras T., Laine S., Aila T. A style-based generator architecture for generative adversarial networks // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. – 2019. – C. 4401-4410.

8. Donahue J., Krähenbühl P., Darrell T. Adversarial feature learning //arXiv preprint arXiv:1605.09782. – 2016.

9. Morris T. H., Thornton Z., Turnipseed I. Industrial control system simulation and data logging for intrusion detection system research //7th annual southeastern cyber security summit. – 2015. – C. 3-4.

АЛАБУГИН Сергей Константинович, аспирант кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sergei_alabugin@mail.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

ALABUGIN Sergei, postgraduate student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sergei_alabugin@mail.ru

SOKOLOV Alexander, Ph.D., Associate professor, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru

Материалы к публикации отправлять по адресу E-mail: urvest@mail.ru
в редакцию журнала «Вестник УрФО. Безопасность в информационной сфере».

Или по почте по адресу: Россия, 454080, г. Челябинск, пр. им. Ленина, д. 76,
ЮУрГУ, Издательский центр.

ВЕСТНИК УрФО
Безопасность в информационной сфере № 4(38) / 2020
Подписано в печать 30.12.2020.
Дата выхода в свет 25.01.2021. Формат 70×108 1/16. Печать цифровая.
Усл.-печ. л. 6,3. Тираж 100 экз. Заказ 453/3.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 4(38) / 2020
Signed to print December 30, 2020.
Date of publication of the 25.01.2021. Format 70×108 1/16. Screen printing.
Conventional printed sheet 6,3. Circulation – 100 issues. Order 453/3. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080