Индекс 79187

ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

1

(140)

Подписывайтесь,

читайте,

пишите в наш журнал

Москва 2023

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

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

Межотраслевой научно-технический журнал

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

Подписной индекс **79379**

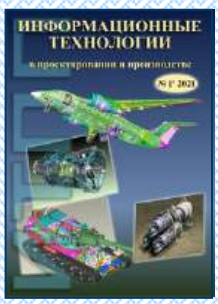
Издается с 1984 года

Межотраслевой научно-технический журнал

Конструкции из композиционных материалов
(4 выпуска)

Подписной индекс **80089**

Издается с 1981 года



Научно-технический журнал

Информационные технологии в проектировании и производстве
(4 выпуска)

Подписной индекс **79378**

Издается с 1976 года

Межотраслевой научно-практический журнал

Экология промышленного производства
(4 выпуска)

Подписной индекс **80090**

Издается с 1993 года

Научно-практический журнал

Вопросы защиты информации
(4 выпуска)

Подписной индекс **79187**

Издается с 1974 года

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

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

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

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

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

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

1 (140)

Москва 2023

Основан в 1974 г.

С О Д Е Р Ж А Н И Е

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2023.
Вып. 1 (140). С. 1—52.

Компьютерная верстка: *Н. В. Ильина*, *К. В. Трыкина*

Подписано в печать 20.03.2023. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 6,0. Уч.-изд. л. 6,2.
Тираж 400 экз. Заказ 2011. Свободная цена.
Адрес редакции: 125424, Москва,
Волоколамское ш., 77. ФГУП «НТЦ оборонного комплекса «Компас».
http://ntckompas.ru
Отпечатано: 101000, Москва,
Лубянский проезд, д. 15, стр. 4, помещ. IX, ком. 15, 16
ООО «Спиди-Принт.ру»
Индекс 79187.

УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004
DOI: 10.52190/2073-2600_2023_1_3
EDN: OFNBUJ

Исследование средств и методов эффективного и качественного обеспечения информационной безопасности в сетях сотовой и подвижной связи

В. В. Кабаков
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Проведен анализ технических средств и особенностей обеспечения качества и безопасности в сетях сотовой подвижной связи на примере резервирования каналов. Предпринята попытка комплексного исследования вопроса и систематизации знаний относительно темы исследования. Предлагается использовать данные материалы в качестве научно-теоретической базы в дальнейших исследованиях, связанных с практической реализацией обеспечения безопасности в сетях сотовой подвижной связи.

Ключевые слова: информационная безопасность, сеть, межсетевой экран, мобильная связь, резервирование каналов, компьютерная сеть.

В современном мире происходит активное развитие и модернизация компьютерных и информационных технологий, в частности, сетей передачи данных. Несмотря на все преимущества, которые даёт использование сетей мобильной связи, на сегодняшний день актуализируются проблемы, связанные с обеспечением ее безопасности. Развитие и обеспечение безопасности в работе таких систем является приоритетом политики Российской Федерации.

Исходя из этого, развитие и внедрение информационных технологий является главным трендом цифровой трансформации современных профессиональных областей жизнедеятельности человека. При этом наиболее значимым вопросом является обеспечение информационной безопасности компьютерных сетей. Происходит активная разработка и интеграция инновационных средств и методов для обеспечения качества и безопасности передачи данных рассматриваемыми средствами [1].

Цель работы — детальное исследование наиболее значимых инструментов решения представленной проблемы.

Кабаков Виталий Валериевич, старший преподаватель.
E-mail: ser-kvv73@mail.ru

Статья поступила в редакцию 4 января 2023 г.

В представленных материалах формируется научно-теоретическая база, использование которой является актуальным при обеспечение безопасности на современных объектах, использующих сети передачи данных. Объект исследования — сотовая подвижная связь. Предметом исследования является вопрос обеспечения информационной безопасности при функционировании данной связи.

Материалы и методы

В исследование использованы теоретические и эмпирические методы и актуальные данные научных работ отечественного и зарубежного авторства [1—8]. В каждой из работ затрагиваются фундаментальные вопросы, необходимые для проведения общего анализа, касающегося информационной безопасности в сетях сотовой подвижной связи.

Таким образом, в данной работе автором рассмотрены такие вопросы, как: современные проблемы и пути обеспечения электромагнитной безопасности сотовой связи, конвергенция сервисов качества и защиты информации в сетях сотовой подвижной связи на этапе проектирования, инновации и информационная безопасность в области технологий сетевой связи и другие.

Актуализация вопроса информационной безопасности в сетях сотовой подвижной связи

В течение последних лет наблюдается резкое увеличение используемых сетей подвижной (мобильной) связи на территории нашей страны и за рубежом. При этом интеграция данных систем происходит не только в целях организации связи между подвижными объектами, где отсутствуют альтернативы таким сетям, но также и для организации связи между некоторыми стационарными объектами. Основной принцип работы подвижной связи заключается в преобразовании и передаче цифровых данных на основе стандарта GSM. Важно отметить, что общая концепция обеспечения безопасности связи GSM основана на технических, организационных и правовых аспектах. Однако для более полной защиты необходимо обеспечить тесное взаимодействие каждого из этих элементов.

Под понятием "безопасность подвижной связи" понимается комплекс средств, мер и действий, в результате функционирования которого производится защита системы от несанкционированного доступа, а также обеспечивается секретность при передаче информации. Меры безопасности таких сетей используют с целью не допустить противоправных действий. При этом данного рода действия зачастую разделяются на два главных аспекта — действия, направленные в целях искажения или перехвата информации, а также действия, направленные для получения бесплатного доступа к сети связи [2].

На рынке подвижной связи присутствуют решения для различных областей жизнедеятельности человека. Так, выделяются профессиональные системы подвижной связи, персональные, беспроводные телефоны, а также сети подвижной связи общего пользования. Особенную актуальность приобретают вопросы обеспечения качества и безопасности передачи информации среди первого вида связи. Профессиональные сети подвижной связи активно используют в военной сфере, промышленности и ряде иных сфер, требующих быстрой и безопасной передачи данных для решения важных задач.

Актуализация вопросов обеспечения безопасности данного вида связи неизбежно привела к разработке рядя решений, позволяющих обеспечить достаточный уровень защиты и качества передачи информации. Одним из инструментов для решения задач из данной области является использование резервирования каналов. Переход на резервный канал производится без потери времени по результатам обнаружения отказа основного канала. При этом возврат после его восстановления выполняется только по результатам проверки надежности [3].

Методы анализа защищенности компьютерных сетей

В связи с высокой степенью необходимости использования компьютерных сетей на современных предприятиях, все большее внимание уделяется вопросу поддержания должного уровня их информационной безопасности. Непрерывное развитие и повсеместное использование сетей порождает рост уязвимостей программных ресурсов. В свою очередь, широкое распространение средств реализации данных угроз актуализирует применение различных систем анализа защищенности.

Данные системы представляют программно-аппаратные средства, направленные на выявление фактов несанкционированного доступа в компьютерную сеть. При этом выделяются три основных типа атаки. Первый из них является подготовительным и заключается в поиске предпосылок для выполнения той или иной атаки. На этом этапе производится поиск уязвимостей, дальнейшее использование которых и приводит к реализации атаки, что является вторым этапом.

На третьем этапе происходит завершение атаки и "заметание" следов. Методы анализа защищенности компьютерных сетей направлены на обеспечение дополнительного уровня защиты компьютерных сетей и разделяются на такие классы относительно позиции в сети, как хостовые и сетевые системы обнаружения вторжений [4].

Необходимо отметить, что обнаружением вторжений занимаются системы анализа защищенности. Таковыми являются различные сканеры безопасности, а также системы поиска уязвимостей. На их основе производятся всесторонние исследования заданных систем для обнаружения уязвимостей, приводящих к нарушениям целостности и информационной безопасности. Наибольший уровень угрозы представляют уязвимости проектирования, обнаружение и устранение которых требует большого труда.

Защищенность представляет собой ключевой показатель эффективности функционирования компьютерных сетей, наряду с показателями надежности, отказоустойчивости, производительности и других. Под защищенностью компьютерных сетей обычно понимается степень адекватности реализованных в ней механизмов по обес-

печению защиты информации, потенциально подверженной рискам, связанным с осуществлением угроз безопасности. Данные угрозы могут нарушать такие свойства информации, как ее конфиденциальность, целостность и доступность [5].

Существует ряд основных методов анализа защищённости компьютерных сетей, предполагающих использование активных и пассивных систем тестирования. Аналитический свод наиболее распространенных методов анализа защищенности сетей представлен в таблице.

Представленные в таблице методы имеют индивидуальные особенности, использование которых в соответствии каждой из них может быть рационально в зависимости от размерности и выполняемых задач компьютерных сетей.

Так, к примеру, аппаратные методы анализа защищенности (ручной анализ конфигурационных файлов, анализ механизмов безопасности организационного уровня) являются наиболее эффективными методами сканирования небольших сетей или при решении задач выявления угроз безопасности на этапе проектирования сетей.

Программные методы позволяют произвести более быстрый анализ защищенности масштабных и территориально-распределенных компьютерных сетей, но требуют использования платных программных продуктов.

Одними из наиболее распространенных программных продуктов, использующихся при реализации программного анализа защищенности компьютерных сетей, являются инструменты, представленные на рис. 1.

Методы анализа защищённости компьютерных сетей

Метод	Описание	Преимущества	Недостатки
Анализ механизмов безопасности организационного уровня	Включает в себя анализ политики безопасности организации и документации по обеспечению режима информационной безопасности. Производится оценка их соответствия существующим требованиям и адекватность реагирования к рискам.	Позволяет выявить несоответствия на начальном уровне построения компьютерной сети.	Долгая обработка данных и информации о рисках нарушения безопасности. Недостаточный уровень автоматизации процессов поиска аномалий.
Ручной анализ конфигурационных файлов	Включает в себя анализ межсетевого экрана, прокси-серверов, на основе которых производится управление межсетевыми взаимодействиями, а также иных критических элементов сетевой инфраструктуры.	Может быть полезен при анализе обеспечения информационной безопасности на объектах, где не существует возможности анализа реальных электронно-вычислительных систем.	Низкая эффективность выявления угроз относительно программных методов.
Сканирование внешних сетевых адресов ЛВС из сети Интернет	Основывается на пингах компьютерной сети в целях выявления внешних IP-адресов. Отображает распределение типов ресурсов по сети для выявления аномалий.	Позволяет произвести анализ защищенности относительно внешних угроз безопасности. Высокая эффективность и скорость выявления аномалий.	Ограничен сканированием внешних ресурсов. Требует использования платного программного обеспечения.
Сканирование ресурсов ЛВС изнутри	Основывается на пингах компьютерной сети в целях выявления внутренних IP-адресов. Отображает распределение типов ресурсов по сети для выявления аномалий.	Позволяет произвести наиболее эффективный анализ защищенности относительно внутренних угроз безопасности.	Ограничен сканированием внутренних ресурсов. Требует использования платного программного обеспечения.
Анализ конфигурации серверов и рабочих станций ЛВС	Производится посредством специализированных программных агентов, выявляющих аномалии и нарушения информационной безопасности сети.	Представляет возможность быстрого и эффективного поиска угроз безопасности на основе использования программных продуктов. Представляет высокую актуальность своего использования для сканирования масштабных и территориально-распределенных компьютерных сетей.	Требует использования дорогостоящего программного обеспечения. Не является рациональным к использованию для небольших компьютерных сетей.

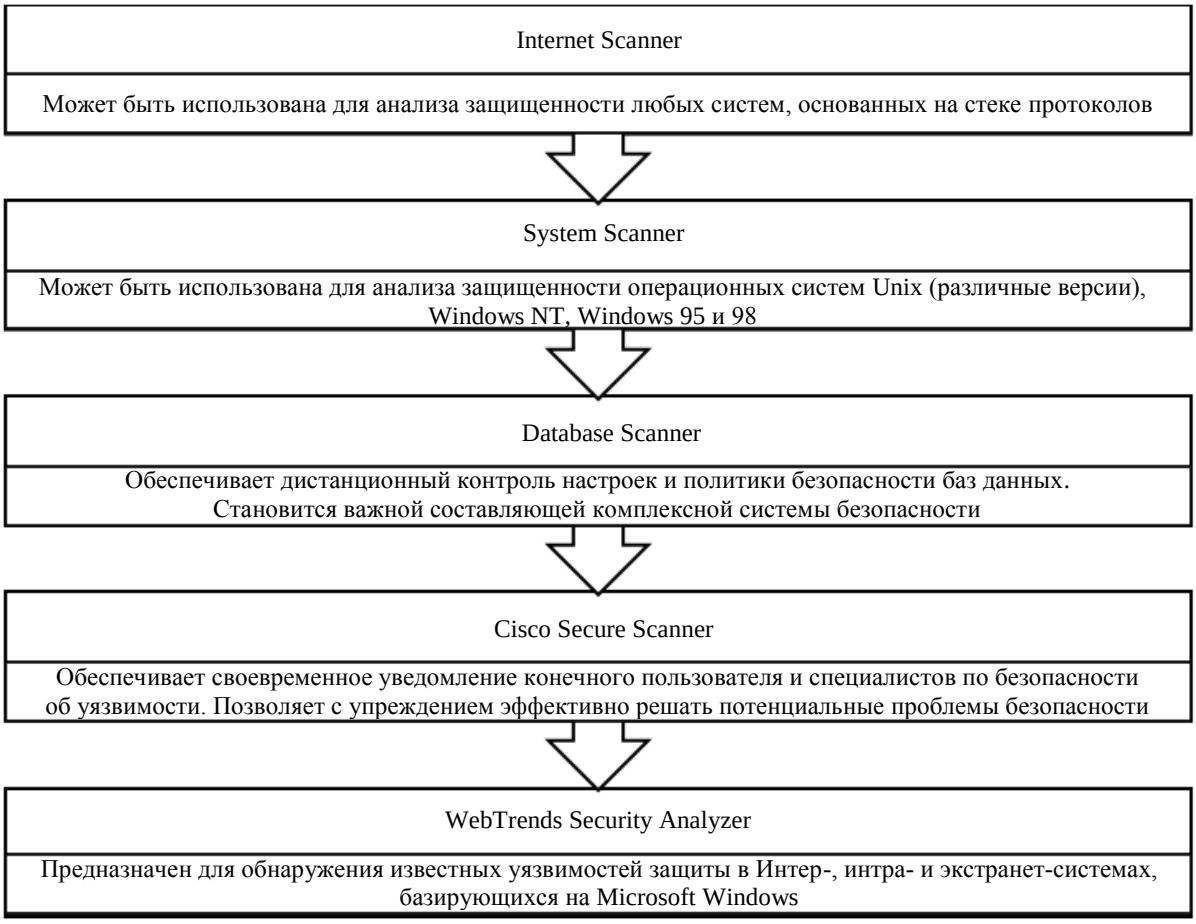


Рис. 1. Средства анализа защищенности компьютерных сетей

Защита сотовой подвижной связи методом резервирования каналов

Необходимо отметить, что наиболее актуальными решениями в вопросах обеспечения безопасности сетей подвижной связи являются интеллектуальные терминалы с резервированием каналов передачи данных. На рис. 2 представлены некоторые из примеров решений данного вида оборудования [6].

Название терминала	Производитель	Описание
Multi-SIM GSM/GPRS Terminal	DIGITAL ANGEL	В продукте реализовано "холодное" резервирование (резервный канал образуется оборудованием при обнаружении неисправности основного канала) беспроводного GPRS-канала передачи с использованием до 4 SIM-карт
Data Terminal & Router	TERMIT	"Интеллектуальное" устройство на базе операционной системы Linux со встроенным сторожевым таймером, поддерживающее различные беспроводные режимы обмена данными
AnCom RM/D	Аналитик-ТС	"Холодное" резервирование беспроводного GPRS-канала передачи с использованием двух SIM-карт и встроенного алгоритма перехода между ними (плюс возможность перехода на CSD)
AnCom RM/E	Аналитик-ТС	"Горячее" резервирование (резервный канал всегда поддерживается в активном состоянии и готов к немедленной передаче данных) с возможностью поддержки проводной (выделенные и коммутируемые каналы, физические линии) и беспроводной (GSM с поддержкой сервисов GPRS или CSD) сред передачи под управлением встроенного контроллера

Рис. 2. Терминалы с резервированием каналов передачи данных

Наиболее актуальным и эффективным решением является модем AnCom RM/E. В зависимости от подключенного объекта данное решение позволяет решать следующие задачи: задачу резервирования каналов связи (по проводному — Ethernet и беспроводному каналу — GSM); задачу коммутации доступа к объекту автоматизации.

Задача резервирования каналов связи с использованием AnCom RM/E решается следующим образом. Удаленный доступ из диспетчерского пункта к объекту, который, в свою очередь, подключен к данному модему (по интерфейсу RS-232/RS-485), производится по Ethernet, то есть основному каналу.

При этом переключение на GSM-канал производится при обрыве проводной связи. Коммутация выполняется в автоматическом режиме с помощью утилиты AnCom Switch RM_E, которая входит в комплект поставки данного технологического решения. На рис. 3 изображена схема работы алгоритма резервирования каналов [7].

В результате работы модема AnCom RM/E создается автоматическая система доступа к интернету. В ней существует не менее двух параллельных каналов связи, дублирующих друг друга. Так, при выходе из строя основного канала происходит автоматическое включение резервного, в результате чего обеспечивается непрерывный доступ в интернет. Это, в свою очередь, позволяет обеспечить наиболее качественную и безопасную передачу данных в сетях сотовой подвижной связи. Основными достоинствами использования данного решения является, непосредственно, сама возможность резервирования каналов, а также наличие интеллектуальной коммутации каналов доступа к объекту.

Одним из актуальных на сегодняшний день применений данного модема является использование в автоматических системах управления наружным освещением (АСУНО). Встроенный в данную систему модем AnCom RM/E позволяет обеспечить устойчивый и безопасный канал удлинения данных с диспетчерским пунктом. Модем выступает решением для повышения надежности передачи данных, требуя при этом подключение к интернету, которое производится на основе двух встроенных SIM-карт. Основной особенностью работы AnCom RM/E в АСУНО является возможность автоматического резервирования каналов для доступа к сети Интернет, при этом во время выхода из строя всех каналов связи модем позволяет перевести работу системы освещения в ручной режим, оповестив при этом оператора соответствующим сигналом через SMS [8].

Так, AnCom RM/E предоставляет возможность обеспечения централизованного оперативного управления АСУНО в ручном и автоматическом режиме. При этом во время сбоев на всех беспроводных каналах связи имеется возможность перехода модема в режим местного управления освещением обслуживающим персоналом с передачей сигналов посредством компьютера через COM порт. Также важно отметить, что ключевая особенность использования рассматриваемого модема состоит не только в возможности удлинения и обеспечения устойчивого (безопасного) соединения, но и в снижении затрат на электроэнергию, техническое обслуживания и ликвидацию аварий. Это достигается в результате формирования на основе собираемых модемом данных, формировании на их основе графиков, возможности производства централизованного учета расхода электроэнергии, проведении дистанционной диагностики оборудования, а также общего повышения надежности АСУНО.

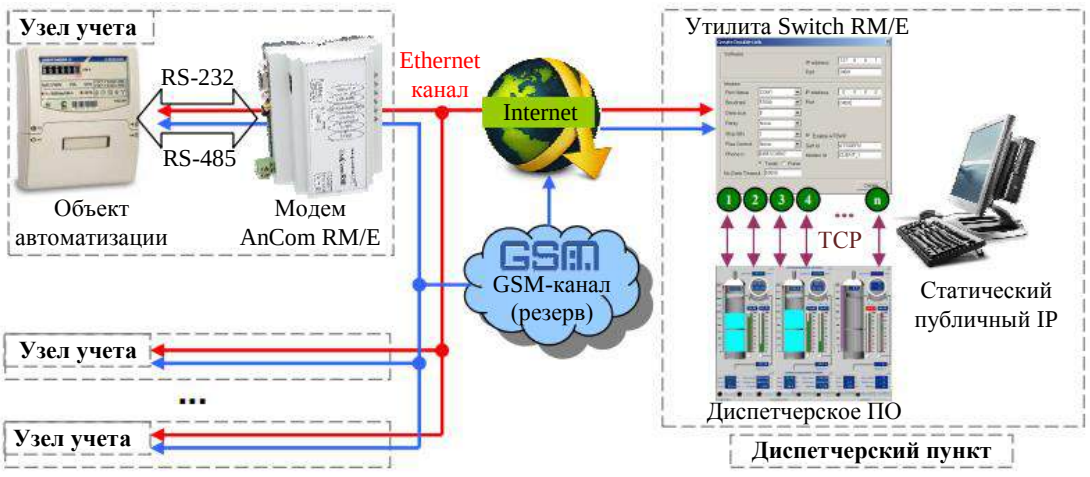


Рис. 3. Алгоритм резервирования каналов с помощью модема AnCom RM/E

Заключение

Основной целью текущей статьи являлось выполнение анализа технических средств и особенностей обеспечения качества и безопасности в сетях сотовой подвижной связи. В качестве примера для анализа вопроса был выбран инструмент резервирования каналов. Необходимо отметить, что существующие технические решения не имеют полной гарантии безопасности от нападений. Исходя из этого, наиболее эффективное обеспечение безопасности в области подвижной связи может быть достигнуто только в результате комплексного решения вопроса, разработки инновационных технических решений, а также непрерывного аудита и анализа возникающих проблем. В результате работы были определены ключевые аспекты и актуальность обеспечения безопасности сетей подвижной связи. Выделен один из наиболее актуальных и эффективных инструментов обеспечения безопасности связи, заключающийся на основе резервирования каналов. Представлен алгоритм работы и выделены основные преимущества использования модема AnCom RM/E при решении данных задач.

Важно подчеркнуть, что вопрос обеспечения информационной безопасности занимает ключевое место в развитии сегмента информационных технологий. При этом ввиду непрерывного появления новых уязвимостей необходимо разрабатывать новые и повышать эффективность существующих инструментов обнаружения угроз и анализа защищенности компьютерных сетей. В заключение необходимо отметить, что реализация мер с использованием модема AnCom RM/E способна значительно повысить качество, надежность и безопасность функционирования систем подвижной связи.

Литература

1. *Рахманин Ю. А., Онищенко Г. Г., Григорьев Ю. Г.* Современные проблемы и пути обеспечения электромагнитной безопасности сотовой связи для здоровья населения // Гигиена и санитария. 2019. Т. 98. № 11. С. 1179—1183.
2. *Бабкин А. Н.* Защита сетей подвижной радиосвязи ОВД от угроз блокирования // Вестник ВИ МВД России. 2019. № 2. С. 165—171.
3. *Максименко В. Н.* Конвергенция сервисов качества и защиты информации в сетях сотовой подвижной связи на этапе проектирования // T-COMM: Телекоммуникации и транспорт. 2018. Т. 12. № 11. С. 57—64.
4. *Alferov S. U.* 5G: characteristics, areas of application, threats to national security // State Service. 2020. V. 22. № 5. P. 56—61.
5. *Дойникова Е. В., Федорченко А. В., Котенко И. В., Новикова Е. С.* Методика оценивания защищенности на основе семантической модели метрик и данных // Вопросы кибербезопасности. 2021. № 1(41). С. 29—40.
6. *Борзенкова С. Ю., Казарина Е. Е.* Анализ методов оценки уровня защищенности информационных систем в процессе их эксплуатации // Известия ТулГУ. Технические науки. 2020. № 5. С. 93—97.
7. *Коцыняк М. А., Спицын О. Л., Иванов Д. А.* Методика оценки устойчивости сети в условиях таргетированной кибернетической атаки // Наукоемкие технологии в космических исследованиях земли. 2018. Т. 10. № 6. С. 76—85.
8. *Грушо А. А., Грушо Н. А., Забежайло М. И., Тимонина Е. Е.* Методы оценки защищенности компьютерных систем информационной поддержки цифровой экономики // International Journal of Open Information Technologies. 2019. Т. 7. № 4. С. 61—66.

Research of means and methods of effective and high-quality information security in mobile communication networks

V. V. Kabakov
Moscow Aviation Institute (National Research University), Moscow, Russia

The purpose of the current article is to analyze the technical means and features of ensuring quality and security in cellular mobile networks using the example of channel redundancy. The author attempts a comprehensive study of the issue and systematization of knowledge about the research topic. The scientific value of the work consists in the possibility of using the presented materials as a scientific and theoretical basis in further research related to the practical implementation of security in cellular mobile networks.

Keywords: information security, network, firewall, mobile communication, channel reservation, computer network.

Bibliography — 8 references. *Received January 4, 2023*

ДОВЕРЕННАЯ СРЕДА

УДК 004.89; 004.056.53
DOI: 10.52190/2073-2600_2023_1_9
EDN: OKAIZO

Биометрическая аутентификация по тепловым изображениям лица на основе преобразователей "биометрия-код"

[1] *С. С. Жумажанова*, канд. техн. наук; [2] *И. Е. Панфилова*;
[1] *А. Е. Сулавко*, канд. техн. наук; [1] *П. С. Ложников*, д-р техн. наук; [1] *А. Е. Серикова*

[1] ФГБОУ ВО «Омский государственный технический университет», г. Омск, Россия
[2] ФГБОУ ВО «Самарский государственный технический университет», г. Самара, Россия

Разработан метод биометрической аутентификации на основе нейросетевых моделей искусственного интеллекта по тепловым изображениям лица в защищенном режиме исполнения. Под "защищенным исполнением" понимается невозможность анализа логики работы искусственного интеллекта, управления искусственным интеллектом и извлечения знаний из его памяти (например, персональных данных) любым неавторизованным лицом. В основе метода лежит искусственная нейронная сеть InceptionResNet, а также модифицированный нейросетевой преобразователь "биометрия-код", обучаемый по ГОСТ Р 52633.5. Результаты показали, что при таком подходе изменение психофизиологического состояния субъекта не приводит к снижению точности аутентификации. Наилучшие показатели ошибок аутентификации составили: EER = 4,91 (FFR = 0,27 при FAR < 0,001). Предложенный метод является робастным по отношению к пользователю и его состоянию, а также работоспособен на малых обучающих выборках (8 примеров термограммы на человека).

Ключевые слова: многослойные нейронные сети, нейросетевые преобразователи "биометрия-код", автоматическое обучение, термограммы лица, биометрическая аутентификация, извлечение признаков, оценка информативности признаков.

Любое несанкционированное вмешательство в работу искусственного интеллекта (ИИ) может повлечь за собой последствия — материальный ущерб, нарушение информационной безопасности, угрозу жизни, здоровья граждан, технологический сбой или катастрофу и т. д. Все зависит от назначения конкретной реализации ИИ и возможностей, которыми данный экземпляр обладает. Поэтому в ответственных приложениях ИИ должен обладать поддержкой защищенного режима исполнения. Под "защищенным исполнением" понимается невозможность анализа логики работы ИИ, управления ИИ и извлечения знаний из памяти ИИ (например, персональных данных) любым неавторизованным лицом.

К ответственным приложениям ИИ относят системы биометрической аутентификации по изображению отпечатка пальца, радужки, рукописного образа, голосу и другим параметрам. Биометрические образы являются персональными данными, которые нуждаются в надежной защите от компрометации. Защищенное исполнение процедуры биометрической аутентификации можно реализовать на базе гомоморфного шифрования либо с помощью специальных моделей — преобразователей "биометрия-код" (ПБК), позволяющих связать биометрический образ человека с его паролем или личным криптографическим ключом. Эти модели можно разделить на две основные категории:

- нечеткие экстракторы (fuzzy extractors, fuzzy commitment, fuzzy vault, fuzzy embedder), основанные на применении кодов, исправляющих ошибки;
- нейросетевые преобразователи "биометрия-код" (НПБК), основанные на применении искусственных нейронных сетей (ИНС).

Цель исследования — разработать и протестировать метод биометрической аутентификации по

Жумажанова Самал Сагидулловна, старший преподаватель.
E-mail: samal_shumashanova@mail.ru
Панфилова Ирина Евгеньевна, аспирант, инженер.
E-mail: panfilova_2015@bk.ru
Сулавко Алексей Евгеньевич, доцент кафедры "Комплексная защита информации".
E-mail: sulavich@mail.ru
Ложников Павел Сергеевич, заведующий кафедрой "Комплексная защита информации".
E-mail: lozhnikov@gmail.com
Серикова Анастасия Евгеньевна, студент.
E-mail: nastya.ser2015@gmail.com

Статья поступила в редакцию 21 декабря 2022 г.

тепловому портрету лица человека в защищенном режиме исполнения на основе преобразователя "биометрия-код".

Большинство биометрических образов уязвимы с точки зрения возможности их фальсификации в целях проведения злоумышленником состязательных атак. В этом отношении тепловые изображения обладают преимуществом, так как подделать тепловой портрет человека (изготовив муляж биометрического образа) для обмана тепловизора затруднительно.

Краткий обзор моделей ПБК и методов реализации защищенного режима исполнения ИИ

1. Гомоморфное шифрование

Гомоморфное шифрование открывает значительные перспективы с точки зрения построения защищенного режима исполнения ИИ. Это форма шифрования, позволяющая производить математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполненных с открытым текстом. Основная проблема этих методов заключается в низкой производительности. Например, в работе [1] речь идет о полном гомоморфном шифровании данных отпечатка пальца для систем пограничного контроля с учетом требований GDPR (General Data Protection Regulation). Сравнение предъявляемых образов с эталонами отпечатка пальца требует значительных вычислительных ресурсов, а распознавание личности даже с использованием параллельных вычислений занимает слишком много времени. В работе [2], по заявлению авторов, предложена первая общая структура для защиты мультибиометрических шаблонов, основанная на гомоморфном шифровании, которая позволяет обрабатывать только зашифрованные данные с учетом выполнения всех требований стандарта ISO/IEC 24745 (Information technology — Security techniques — Biometric information protection). Однако авторы отмечают, что главный недостаток схемы — низкое быстродействие. Даже для простых решающих правил снижение производительности значительно.

Распознавание образов в защищенном с помощью гомоморфного шифрования режиме имеет тенденцию к повышению количества ошибочных решений. В частности, в [3] предложен метод гомоморфной защиты параметров лиц, извлекаемых из изображений с помощью глубоких нейронных сетей. Извлекаемые параметры шифруются с помощью вероятностной криптосистемы Пэйе. Предложенная схема шифрования снижает точность верификации лиц. Ситуация может объясняться тем, что гомоморфные шифротексты перестают расшифровываться после выполнения достаточно большого числа операций сложения и умножения.

Эти проблемы могут быть решены в будущем, однако эффективная защита биометрических шаблонов возможна и без использования гомоморфного шифрования.

2. Нечеткие экстракторы

В схемах fuzzy extractor (fuzzy commitment, fuzzy vault, fuzzy embedder) на ключ накладывается помехоустойчивый код (БЧХ, Рида-Соломона, Адамара), далее ключ объединяется с биометрическими характеристиками и формируется закрытая строка. В процессе аутентификации субъект предъявляет биометрические данные, которые "вычитаются" из закрытой строки для получения ключа. Если в ключе есть небольшое количество неверных бит, применяется алгоритм исправления ошибок. Этот подход имеет принципиальные недостатки:

- длина ключа в классической схеме нечеткого экстрактора зависит от исправляющей способности помехоустойчивого кода. Чем выше исправляющая способность, тем больше избыточности содержится в закрытой строке и меньше длина ключа. Использовать схему по отношению к слабым биометрическим данным затруднительно, так как в этом случае нужно исправлять большое количество бит ключа;
- нечеткие экстракторы представляют собой слабые решающие правила (они не способны к полноценному обучению и не анализируют данные, так, как это делают нейронные сети). Нечеткий экстрактор может работать при относительно низкой длине ключа *len*, если на его входы поступают высокоинформативные биометрические параметры, например, радужки (*len* = 70 бит [4]) или отпечатка пальца ($48 \le len \le 64$ бит [5]). При обработке рукописных образов показатели FRR, FAR оказываются очень высокими (например, FAR = 0,2 % при FRR = 76,53 % или FAR = 6,91 % при FRR = 7,85 % [6]).

Нечеткие экстракторы часто объединяют с предварительно обученными глубокими нейронными сетями, которые извлекают из образа более информативные признаки. Результат такого объединения не стоит относить к принципиально новым схемам, так как при этом наследуются недостатки классической схемы. Единственным улучшением является более эффективный блок

извлечения признаков. Примером является работа [7], в которой из параметров походки человека генерировался ключ длиной 128 бит (против 50 бит в [8], где в аналогичной задаче использовали схему fuzzy commitment без нейросети).

3. Нейросетевые преобразователи "биометрия-код"

Первая модель of neuro-extractor была разработана как основа российского государственного стандарта ГОСТ Р 52633.5-2011 [9]. Эта модель представляла собой shallow neural network, состоящую из одного или двух скрытых частично связных слоев, которая обучалась по робастному автоматическому алгоритму (без применения градиентного спуска). ANN кодирует знания об особенностях биометрических образов весовыми коэффициентами, что не позволяет напрямую наблюдать за биометрическими параметрами. Первый neuro-extractor имел пороговую функцию активации нейронов для извлечения бинарного кода ключа. Он строился персонально для каждого пользователя и работал в режиме верификации (сравнение один к одному), для обучения требовались примеры образов "Свой" и "Чужие", а также криптографический ключ. Neuro-extractor можно объединить с глубокой нейронной сетью, и он позволяет извлекать ключи большей длины с меньшим количеством ошибок по сравнению обычным fuzzy extractor (в [10] сообщается, что из рукописных подписей удалось извлечь ключи длиной 256 бит при сравнительно низких показателях ошибочных решений). Однако классическая схема of neuro-extractor имеет проблемы утечки конфиденциальности. Известна атака Маршалко [11], которая базируется на анализе весовых коэффициентов и таблиц связей нейронов, а также другие состязательные атаки, направленные на извлечение знаний из neuro-extractor путем наблюдения статистик его входов/выходов во время работы [12].

В [13, 14] предложены модели deep neuro-extractors на основе многослойных сверточных нейронных сетей для приложений лицевой биометрии. ANN из [13] имеет два сверточных слоя, слой MaxPooling, два полносвязных слоя и два слоя Dropout. Показатели ошибок составили: FAR = 1 % при FRR = 2,41 % при длине ключа 1024 бит (на наборе данных PIE). В работе [14] используется ансамбль (стек) из двух нейронных сетей. Первая сеть VGG-Face (13 сверточных и 2 полносвязных слоя) предварительно обучена на 2,6 млн примеров и принимает на вход изображения лиц 224×224, а на выходе выдает 4096-битный бинарный код. Вторая сеть (6 полносвязных слоев, обучаемых оптимизатором Adam) переводит 4096-битный вектор в ключ пользователя, который задается при ее обучении и имеет длину до 1024 бит, тем самым устраняется корреляция между исходным изображением и ключом. Коэффициент равной вероятности ошибок (FAR = FRR) составил EER = 3,6 %. Недостаток схемы deep neuro-extractor связан с тем, что алгоритмы на базе градиентного спуска имеют склонность к переобучению. Из-за этого схема может плохо переноситься на другие модальности, так как структура образов и архитектура ANN для каждой модальности различны. Хотя авторам работы [14] удалось сделать обучение робастным, для другой модальности робастность не гарантирована.

Классификаторы на базе глубоких сверточных сетей с функцией SoftMax на выходе уязвимы перед состязательными атаками [15]. Известно, что наложение аддитивного Гауссовского шума на изображение существенно увеличивает FAR при верификации биометрических образов с помощью нейронных сетей с подобной архитектурой [16]. Доступ к весовым коэффициентам существенно упрощает подобные атаки. Поэтому архитектура neuro-extractor должна строиться так, чтобы веса синапсов не компрометировали биометрические данные пользователей.

Последние достижения в области построения НПБК изложены в работе [16]. Предложена новая модель НПБК — correlation based neuro-extractor (c-neuro-extractor), основанная на разностных корреляционных нейронах Байеса-Минковского, которая не имеет ограничений, характерных для существующих моделей, но имеет ряд преимуществ, позволяющих использовать для аутентификации более длинные ключи (пароли), а также снизить вероятность ошибок "ложного отказа" (FRR) и "ложного принятия" (FAR). Корреляционные нейроны — это новый класс нейронов, анализирующих корреляционные связи между признаками вместо значений признаков в задачах классификации образов. Анализ внутренних корреляционных связей образов и принятие классификационных решений происходят без необходимости хранения информации о корреляционных связях или значениях признаков, характерных для биометрических образов пользователей. Другими словами, эталонная информация о классах образов не компрометируется при хранении. Процесс обучения корреляционных нейронов полностью автоматический и сохраняет робастность даже на малых обучающих выборках.

В данной работе применялся модифицированный НПБК, основанный на ГОСТ Р 52633.5-2011.

Набор данных термограмм лица

При разработке данного метода аутентификации авторами был сформирован набор данных термограмм лиц 90 испытуемых, которые находились в следующих психофизиологических состояниях (ПФС):

- нормальное (перед съемкой субъект не подвергался каким-либо воздействиям);
- после физической нагрузки (бег, отжимания), объем которой рассчитывался индивидуально;
- алкогольное опьянение в трех различных стадиях: 0,2—0,29 ‰; 0,3—0,59 ‰; 0,6—0,9 ‰ (субъект принимал алкоголь в дозировке, рассчитанной индивидуально по формуле Видмарка, далее через 30 минут участвовал в записи видео, постепенно увеличивая дозировку).

Для записи использовали тепловизор FLIR A615, имеющий детектор разрешением 640×480 пикселей, оптическое поле зрения — 25°×18,8°, термочувствительность — 0,05°, температурный диапазон –20 + 650 °C. В каждом состоянии для каждого субъекта было записано по 10 видеозаписей, длительностью 20—30 секунд. Подробнее с указанными состояниями и их выбором можно ознакомиться в публикациях [17].

Каждый испытуемый подписал согласие на участие в эксперименте и согласие на обработку персональных данных. Далее набор данных был обезличен.

Были рассмотрены основные этические проблемы создания и внедрения технологий на базе ИИ с учетом того, что создаваемые метод и программно-аппаратный комплекс требуют непосредственного участия людей в сборе их данных, а также документы, регулирующие вопросы создания таких систем. Ключом к созданию доверенных систем биометрической аутентификации является соблюдение этических принципов, например, безопасность, робастность, устойчивость, предвзятость, законность и др.

Общая структура системы аутентификации по тепловому изображению лица

Системы идентификации и аутентификации субъектов по лицу, детектируемому на тепловых и обычных изображениях, строятся по схожему шаблону. Входные данные в системе распознавания лиц — это всегда изображение или видеопоток. Система распознавания лиц обычно определяется как процедура, состоящая из трех основных шагов: нахождение лица на изображении (детекция лица), извлечение признаков и распознавание лица, первые два из которых могут выполняться одновременно.

Нахождение (детектирование) лиц определяется как процесс извлечения лиц из изображения или видеопотока. Методы детекции лиц условно можно разделить на две категории: на методы, основанные на антропометрических знаниях о человеческих лицах, и методы определения лиц с предварительным обучением. Методы первой категории являются весьма ограниченными, так как большая проблема заключается в сложности создания соответствующего набора правил (невозможно найти много лиц на сложном изображении). Вторая категория включает специальные методы (например, Eigenface), подход на основе статистических распределений, подход на базе ИНС, которые могут быть использованы на любом из этапов — от определения места расположения лица до распознавания образа объекта в уже имеющемся пространстве признаков.

Этап извлечения признаков включает в себя получение соответствующих черт лица. На этом этапе подразумевается, что проблема определения фрагмента изображения, на котором находится лицо, решена. Процесс извлечения признаков может состоять из нескольких подэтапов: непосредственно извлечение значений признаков (feature extraction) и выбор наиболее информативных из них (feature selection), т. е. уменьшение размерности пространства признаков.

Особое распространение для задач распознавания и идентификации/верификации лиц сегодня получили методы на основе нейронных сетей, а точнее глубоких нейронных сетей [18]. По сравнению с другими подходами эти методы позволяют быстрее и эффективнее работать с изображениями. Существует два распространенных подхода использования глубокого обучения для систем распознавания лиц.

1. Решения с предварительно обученными моделями. Подобные модели уже имеют набор алгоритмов для распознавания различных объектов, в том числе и лиц.

2. Обученная "с нуля" ИНС. Такие сети подходят для сложных систем распознавания лиц с многоцелевой функциональностью. При таком подходе архитектура нейросети также может быть разработана исследователем либо за основу может быть взята существующая архитектура (как с изменениями, так и без). Разработка и обучение ИНС занимают гораздо больше времени и требует огромного количества изображений для обучающего набора данных.

Широкое распространение имеют сверточные нейронные сети (CNN) [19], лучше всего зареко-

мендовавшие себя в задачах распознавания графических образов на изображениях. Существует большое число архитектурных реализаций сверточных сетей (ResNet, XResNet, AlexNet, InceptionResnet, VGGNet и др.). Однако не все из них распространяются в качестве реализаций с открытым исходным кодом и подходят для задач верификации личности по лицу.

Спецификой построения системы распознавания личности именно по тепловому изображению лица является то, что существующие решения для детекции лиц и извлечения признаков обучены и протестированы на обычных изображениях лиц. Если существующее решение чувствительно к цвету изображения — оно не будет работать для термограмм, так как цветовая схема теплового изображения имеет принципиально иную структуру. Решения, основанные на яркости пикселей, также могут работать с более низкой производительностью.

Наконец, система распознает (узнает) человека по лицу. Эта фаза сводится к классификации образов. В задаче идентификации система сообщает идентификатор из базы данных (сравнение "один ко многим"), при аутентификации система подтверждает подлинность аутентификатора (сравнение "один к одному" — верификация). НПБК работает в режиме аутентификации и фактически верифицирует биометрический образ по набору признаков, извлеченных из изображения лица на предыдущем этапе. НПБК для термограмм не имеет значимых отличий от НПБК для обычного изображения.

Детекция лиц на тепловом изображении и извлечение признаков

Одной из библиотек с открытым исходным кодом, включающих в себя этапы детекции и распознавания лиц, является facenet-pytorch. Таким образом, библиотека включает в себя два модуля:

1. Модуль детекции лиц, представленный в виде предобученной сверточной нейронной сети типа MTCNN (Multi-Task Convolutional Neural Network) [20].

2. Модуль распознавания лиц и выделения из них значимых признаков, представленный в виде предобученной сверточной нейронной сети типа InceptionResnet v1.

Первый модуль, а именно многозадачные каскадные сверточные сети (MTCNN) — это фреймворк, разработанный как решение для детекции лиц и их центрирования относительно изображения. Процесс детекции состоит из трех подэтапов, каждый из которых реализуется отдельной CNN (P-Net, R-Net и O-Net).

P-Net реализует технику bounding box regression (BBR), которая используется для локализации на изображении объектов известного класса (в данном случае лиц), ограниченных прямоугольником. Результатом этого этапа являются окна-кандидаты, включающие в себя лицо человека.

Все окна-кандидаты с первого этапа передаются в R-Net. Эта сеть уменьшает количество окон-кандидатов, выполняет калибровку с помощью BBR и объединяет перекрывающиеся окна-кандидаты. R-Net выводит вектор из 4 элементов, который определяет положение и размер ограничивающего прямоугольника, и вектор из 10 элементов локализации ориентира лица.

Сеть O-Net еще более подробно "описывает" лицо человека и выводит вектор пяти точек лицевых ориентиров (два глаза, нос и рот).

В результате работы первого модуля, сеть среди прочего возвращает тензор (терминология PyTorch) с векторами точек детектированного лица, который передается на вход второму модулю — сверточной нейронной сети, построенной на основе архитектуры Inception-ResNet [21] (гибрид Inception и ResNet, рис. 1). Существует две версии Inception-ResNet. Вторая версия дает более высокую потенциальную точность, но требует более высоких вычислительных затрат.

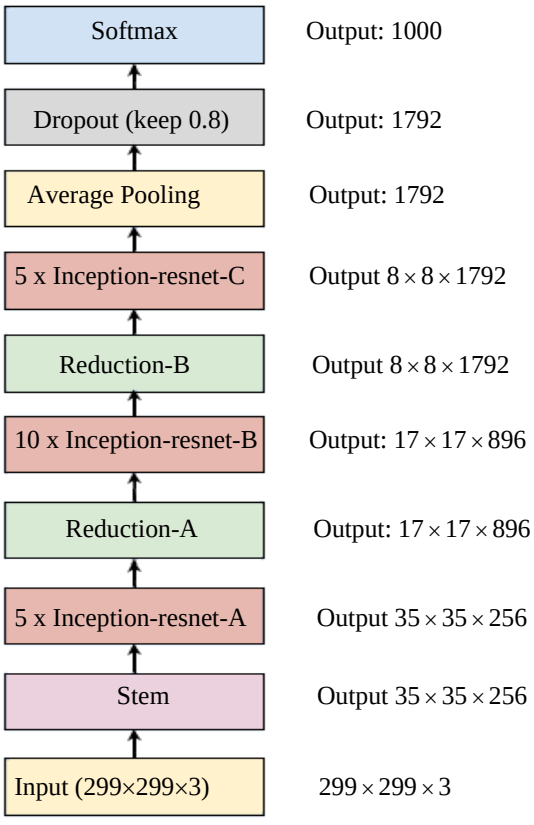


Рис. 1. Архитектура Inception-ResNet (версия 1)

Результатом работы Inception-ResNet является вектор из 512 признаков, выделенных из лица человека.

В основе любых достижений в области нейросетевых технологий и задач компьютерного зрения в области распознавания человеческих лиц лежат многочисленные объемные наборы данных с различными функциями и фокусами [22]. Отметим, что сеть InceptionResNet v.1 имеет две реализации, предобученные на наборе данных VGGFace2 (содержит 3,31 млн изображений 9131 субъекта, в среднем 362,6 изображения для каждого субъекта) и на наборе CASIA-Webface (содержит 494414 изображений лиц 10575 реальных субъектов).

В целях использования рассмотренной библиотеки распознавания лиц для извлечения признаков из тепловизионных изображений лиц, необходимо произвести ряд изменений с имеющимся набором данных термограмм человеческих лиц.

Первый этап изменений заключается в преобразовании изображений в их негатив (рис. 2), что подразумевает инверсию не только цвета, но и яркости. Такое преобразование возможно осуществить с помощью открытой библиотеки для работы с изображениями PIL для языка Python. Эта операция позволила повысить производительность детекции лиц, так как негатив теплового изображения имеет более близкое распределение яркости пикселей к распределению яркости на обычном изображении.

Второй этап преобразований заключается в конвертации полученных негативов в обесцвеченный формат, представленный градациями серого цвета. Такое представление изображения позволяет сделать его более компактным и удобным для обработки сверточными нейронными сетями. Кроме того, реализация конвертации изображения в градацию серого осуществляется с помощью той же библиотеки PIL (изображения именно такого типа ожидает модуль детекции), которая использует преобразование яркости ITU-R 601-2.

После всех проведенных преобразований негативы в градациях серого подаются на вход нейронной сети, извлекающей лица и признаки. В результате на каждой тепловой видеозаписи удалось найти такой кадр, на котором четко было детектировано лицо, и извлечь вектор признаков.

Оценка информативности признаков

Важным показателем является уровень информативности признаков. Количество собственной информации j-го признака для определенного класса образов определяется по формуле (1):

$$I_j = -\log_2\left(AUC\left(\Phi_G\left(a_j\right), \Phi_I\left(a_j\right)\right)\right), \qquad (1)$$

где AUC — площадь (area under curve), ограниченная функциями плотности вероятности "Свой" $\Phi_G(a_j)$ и "Чужие" $\Phi_I(a_j)$, а также осью абсцисс (рис. 3). $\Phi_G(a_j)$ характеризует значения признака строго для определенного класса образов, $\Phi_I(a_j)$ характеризует значения этого же признака для всех остальных классов образов. Чем выше I в среднем, тем дальше разнесены собственные области классов в пространстве признаков и тем признаки информативнее.

При помощи InceptionResNet v.1 из образов были извлечены признаки (каждая термограмма преобразована в 512 признаков). Далее проведена оценка информативности признаков (рис. 4).

Как можно видеть распределение информативности по признакам почти равномерное, это обусловлено нейросетевым характером обработки изображений. Преимуществом экстракторов признаков на основе ИНС является стремление нейросети равномерно распределить информацию между выходами.

Рис. 2. Термограмма лица:
в исходном виде (слева), негатив (в середине), негатив в градациях серого (справа)

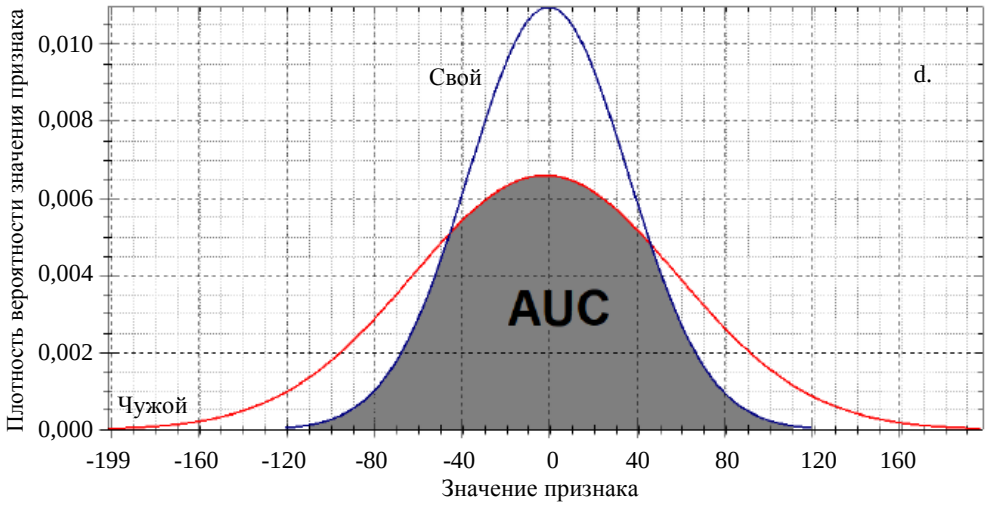


Рис. 3. Оценка информативности признака

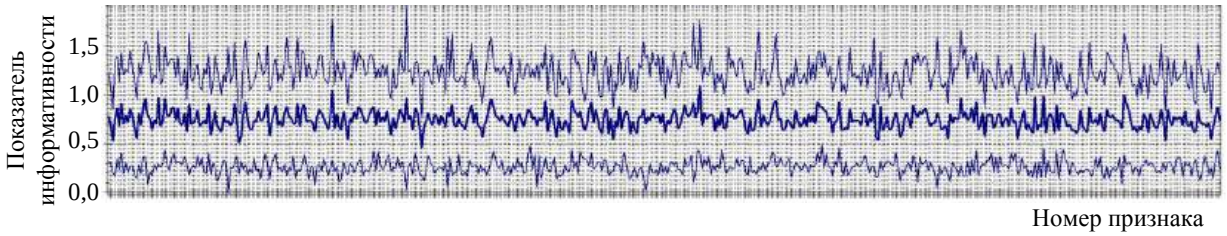


Рис. 4. Информативность признаков (жирная линия — математическое ожидание I, тонкая — математическое ожидание ± стандартное отклонение I)

Реализация нейросетевого преобразователя биометрия-код

Классический однослойный НПБК, обучаемый по ГОСТ Р 52633.5, описан в работах [23]. Нейрон частично связный базируется на функционале взвешенного суммирования и пороговой функции активации. При обучении НПБК задается количество нейронов N и входов нейронов n, номера связанных с нейроном признаков определяются случайно, избегая повторного вхождения признаков в нейрон. Введем параметр I_{min}, который отвечает за информативность признаков. Все признаки, информативность которых ниже I_{min} не учитываются при синтезе и обучении НПБК. Отметим, что информативность признаков для каждого субъекта различна, поэтому для каждого пользователя набор признаков отличается при $I_{min} > 0$. Веса нейронов вычисляются по формуле (2), а нулевой вес (порог) по формуле (3) [24].

$$\mu_j = m_s(a_j) - m_o(a_j) \big/ \sigma_s(a_j)\sigma_o(a_j), \qquad (2)$$

$$\mu_0 = m_s(y), \qquad (3)$$

где y — отклик нейрона на образ "Свой" или "Чужой";

a_j — значение j-го признака (входа нейрона);

$m_o(a_j)$ и $\sigma_o(a_j)$ — математическое ожидание и среднеквадратичное отклонение значений j-го признака для образа "Свой";

$m_s(a_j)$ и $\sigma_s(a_j)$ — аналогичные показатели образов для "Чужих".

Порог нейрона равен математическому ожиданию откликов нейрона на обучающие образы "Чужих", не использовавшиеся при настройке весовых коэффициентов μ_j. Если нейрон настроен на выход "1" при поступлении образа "Свой", то знак весового коэффициента μ_j инвертируется. Если нейрон настраивается на "нулевой" бит, то знак порога μ_0 инвертируется.

Далее к весам нейрона добавляется случайный шум ($\pm 0{,}001\mu_j$). После обучения параметры $m_o(a_j)$, $\sigma_o(a_j)$, $m_s(a_j)$, $\sigma_s(a_j)$ удаляются, чтобы не компрометировать эталон. Остаются таблицы связей и весов μ, которые называют *нейросетевым контейнером*.

Результаты эксперимента

Надежность биометрических систем определяется вероятностью ошибок "ложного отказа"

(FRR) и "ложного принятия" (FAR). Эти показатели связаны. При изменении порога принятия образа баланс вероятностей FRR и FAR изменяется. При равном соотношении FRR = FAR = EER говорят о коэффициенте равной вероятности ошибок (измеряемом также вероятностью или процентом). В данном случае в качестве порога выступает расстояние Хемминга от генерируемого с помощью НПБК бинарного кода до верного ключа пользователя (рис. 5). Этот порог можно изменять, увеличивая или уменьшая корректирующую способность кода, исправляющего ошибки на выходе НПБК.

При проведении эксперимента все испытуемые были разделены на 2 категории случайным образом: "Зарегистрированные пользователи" (65 субъектов) и "Злоумышленники" (25 субъектов). Для каждого зарегистрированного пользователя формировали НПБК, обучаемый на 8 примерах образа "Свой" и 64 примерах образов "Чужие" (по одному от каждого другого зарегистрированного пользователя). Остальные образы "Свой" субъектов использовали при тестировании для вычисления FRR. Образы из категории "Злоумышленники" использовали для оценки FAR. После чего вычислялся коэффициент EER. Данную процедуру повторяли 10 раз и каждый раз испытуемых делили на две категории случайным образом.

Описанную процедуру повторяли при различных параметрах I_{min}, n, N. Результаты эксперимента представлены в таблице.

Балансировка вероятностей FRR и FAR (настройка НПБК) выполняется путем применения кодов, исправляющих ошибки, по отношению к выходным состояниям нейронов. В качестве таких кодов можно использовать коды Безяева, разработанные специально для биометрии [25].

Как можно видеть, наилучшие результаты EER = 4,91 (возможна настройка НПБК для приведения к вероятностям FFR = 0,27 при FAR < 0,001) достигаются при $I_{min} = 0{,}5$, $n = 4$, $N = 256$. При $I_{min} = 0$ используются все признаки, однако многие из них являются шумовыми для отдельных субъектов и не несут полезной информации. Значение $I_{min} = 0{,}5$ оптимально, поскольку в этом случае неинформативные признаки отсеиваются и не используются при обучении и распознавании пользователей. При $I_{min} > 0{,}5$ вероятность ошибки возрастает, что означает, что отсеиваются уже полезные признаки. Наименьшее количество входов нейрона дает меньшие показатели EER, однако дальнейшее снижение n может негативно сказаться на безопасности биометрического шаблона (слишком малое количество входов нецелесообразно). Длина ключа, равная 256 бит, достаточна для практических целей, при таком числе нейронов достигаются лучшие результаты.

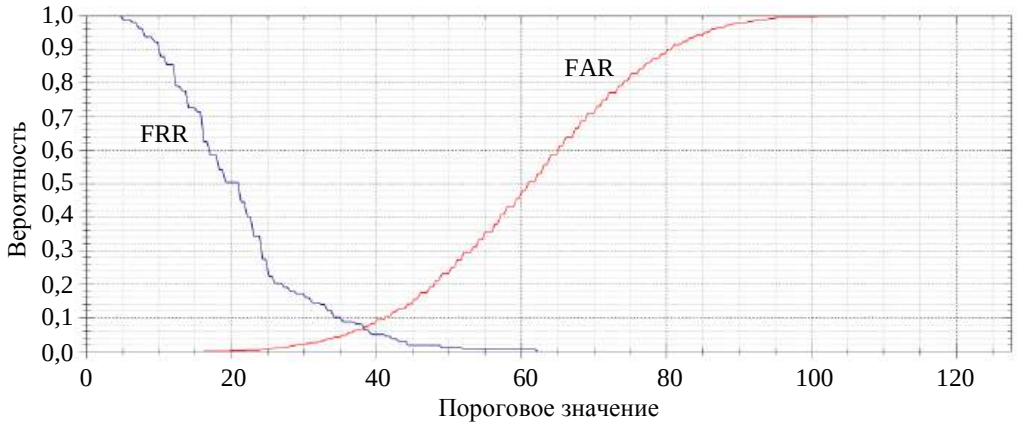


Рис. 5. Балансировка вероятностей ошибок при $I_{min} = 0$, $N = 0$, $n = 0$

Полученные оценки коэффициента равной вероятности ошибок (EER, %)

I_{min}	0		0,25			0,5			0,75		1	
N	128	256	128	256	512	128	256	512	128	256	128	256
n												
4	7,28	6,43	5,81	6,12	6,52	5,77	4,91	5,63	5,42	5,59	6,27	5,59
6	6,4	6,9	6,05	6,93	6,38	5,44	5,1	5,27	6,3	5,52	7,21	7,09
8	7,2	7,2	6,59	6,55	6,24	5,99	6,65	5,8	6,0	6,55	8,17	7,2
10	6,9	6,3	6,35	6,0	5,78	6,76	6,11	5,85	6,97	6,5	7,45	6,97
12	7,72	6,56	7,3	6,65	6,21	6,98	6,35	5,75	7,0	7,0	8,0	7,82

Заключение

В настоящем исследовании разработан метод биометрической аутентификации по тепловым изображениям лица в защищенном режиме исполнения. Это означает, что метод устойчив к таким деструктивным воздействиям, как состязательные атаки и зондирование моделей ИИ. В основе метода лежит сеть InceptionResNet v.1, извлекающая признаки из термограмм (которые предварительно преобразуются в негатив, а потом в изображение в градациях серого), а также модифицированный НПБК, обучаемого по ГОСТ Р 52633.5. Результаты показали, что при таком подходе изменение психофизиологического состояния субъекта не приводит к снижению точности аутентификации (при обучении НПБК использовались данные нормального состояния, при тестировании, как нормального так и измененного). Наилучшие показатели ошибок аутентификации составили: EER = 4,91 (FFR = 0,27 при FAR < 0,001). Предложенный метод является робастным по отношению к пользователю и его состоянию, а также работоспособен на малых обучающих выборках (8 примеров термограммы на человека).

Дальнейшие направления исследований будут связаны с применением и адаптацией моделей НПБК, базирующихся на корреляционных нейронах [17], и гибридных моделей НПБК.

Литература

1. *Catak F. O., Yildirim Yayilgan S., Abomhara M.* Privacy-Preserving Fully Homomorphic Encryption and Parallel Computation Based Biometric Data Matching // Rreprints. 2020. P. 2020070658. DOI: 10.20944/preprints202007.0658.v1.
2. *Gomez-Barrero M. et al.* Multi-biometric template protection based on Homomorphic Encryption // Pattern Recognition. 2017. V. 67. P. 149—163.
3. *Ma Y., Wu L., Gu X. et al.* A secure face-verification scheme based on homomorphic encryption and deep neural networks // IEEE Access. 2017. V. 5. P. 16532—16538.
4. *Rathgeb C., Tams B., Wagner J., Busch C.* Unlinkable improved multibiometric iris fuzzy vault // EURASIP J. Information Security. 2016. V. 1. P. 26.
5. *Hine G. E., Maiorana E., Campisi P.* A zero-leakage fuzzy embedder from the theoretical formulation to real data // IEEE Transactions on Information Forensics and Security. 2017. V. 12(7). P. 1724—1734.
6. *Ponce-Hernandez W., Blanco-Gonzalo R., Liu-Jimenez J., Sanchez-Reillo R.* Fuzzy vault scheme based on xed-length templates applied to dynamic signature verification // IEEE Access. 2020. V. 8. P. 11152—11164.
7. *Sun Y., Lo B.* An artificial neural network framework for gait-based biometrics // IEEE J. biomedical and health informatics. 2018. V. 23(3). P. 987—998.
8. *Elrefaei L. A., Mohammadi Al. A.* M. Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme // J. King Saud University-Computer and Information Sciences. 2019. URL: https://www.sciencedirect.com/science/article/pii/S1319157819300916 (date accessed: 07.04.2021). https://doi.org/10.1016/j.jksuci.2019.10.011.
9. *Akhmetov B., Doszhanova A., Ivanov A. et al.* Biometric Technology in Securing the Internet Using Large Neural Network Technology // World Academy of Science, Engineering and Technology. 2013. V. 7. № 7. P. 129—139.
10. *Malygin A., Seilova N., Boskebeev K., Alimseitova Z.* Application of artificial neural networks for handwritten biometric images recognition // Computer Modelling and New Technologies. 20177. V. 21(1). P. 31—38.
11. *Marshalko G. B.* On the security of a neural network-based biometric authentication scheme // Matematiceskie voprosy kriptografii. 2014. V. 5. № 2. P. 87—98. DOI: https://doi.org/10.4213/mvk120.
12. *Bogdanov D. S., Mironkin V. O.* Data recovery for a neural network-based biometric authentication scheme // Математические вопросы криптографии. 2019. Т. 10. № 2. С. 61—74. DOI: https://doi.org/10.4213/mvk284.
13. *Pandey R. K., Zhou Y., Kota B. U., Govindaraju V.* Deep secure encoding for face template protection // IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). 2016. P. 77—83. DOI:10.1109/CVPRW.2016.17
14. *Jindal A. K., Chalamala S., Jami S. K.* Face template protection using deep convolutional neural network // IEEE Conference on Computer Vision and Pattern Recognition Workshops. — Salt Lake City, UT, USA, 2018. P. 462—470.
15. *Alcorn M. A. et al.* "Strike (With) a Pose: Neural Networks Are Easily Fooled by Strange Poses of Familiar Objects," 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2019. P. 4840—4849. DOI: 10.1109/CVPR.2019.00498.
16. *Hafemann L. G., Sabourin R., Oliveira L. S.* Characterizing and evaluating adversarial examples for Offline Handwritten Signature Verification // IEEE Transactions on Information Forensics and Security. 2019. V. 14. I. 8. P. 2153—2166. DOI: 10.1109/TIFS.2019.2894031.
17. *Sulavko A.* Biometric-Based Key Generation and User Authentication Using Acoustic Characteristics of the Outer Ear and a Network of Correlation Neurons // Sensors. 2022. V. 22. P. 9551. https://doi.org/10.3390/s22239551.
18. *Thai Hoang Le.* Applying Artificial Neural Networks for Face Recognition. Hindawi Publishing Corporation Advances in Artificial Neural Systems Volume 2011. 2011
19. *Wang Jie, Li Zihao* Research on Face Recognition Based on CNN // IOP Conf. Series: Earth and Environmental Science. 2018. P. 170.
20. *Zhang K., Zhang Z., Li Z., Qiao Y.* Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks // Computer Vision and Pattern Recognition (cs.CV). 2016. DOI: 10.1109/LSP.2016.2603342.
21. *Qi X., Zhang L.* Face Recognition via Centralized Coordinate Learning // Computer Science. 2018.
22. *Baojin Huang, Zhongyuan Wang, Guangcheng Wang, Kui Jiang, Zheng He, Hua Zou, Qin Zou* Masked Face Recognition Datasets and Validation. 2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW). 2021.
23. *Сулавко А. Е., Иниватов Д. П., Стадников Д. Г., Чобан А. Г.* Преобразователь образов голосовых паролей дикторов в криптографический ключ на основе комитета предварительно обученных сверточных нейронных сетей // Вопросы защиты информации. 2021. № 4. С. 23—33.
24. *Сулавко А. Е.* Высоконадежная аутентификация по рукописным паролям на основе гибридных нейронных сетей с обеспечением защиты биометрических эталонов от компро-

метации // Информационно-управляющие системы. 2020. № 4. С. 61—77. DOI: 10.31799/1684-8853-2020-4-61-77.

25. *Безяев А. В., Иванов А. И., Фунтикова Ю. В.* Оптимизация структуры самокорректирующегося био-кода, хранящего синдромы ошибок в виде фрагментов хеш-функций // Вестник УрФО. Безопасность в информационной сфере. 2014. № 3(13). С. 4—13.

Biometric authentication based with thermal facial images based on biometrics to code converters

[1] *S. S. Zhumazhanova,* [2] *I. E. Panfilova,* [1] *A. E. Sulavko,* [1] *P. S. Lozhnikov,* [1] *A. E. Serikova*

[1] Omsk State Technical University, Omsk, Russia
[2] Samara State Technical University, Samara, Russia

In the present study, a biometric authentication method was developed based on artificial intelligence neural network models based on thermal facial images in a protected execution mode. "Protected execution" means the impossibility of analyzing the logic of the work of artificial intelligence, controlling artificial intelligence and extracting knowledge from its memory (for example, personal data) by any unauthorized person. The method is based on the artificial neural network InceptionResNet, as well as a modified biometrics-code neural network converter trained according to GOST R 52633.5. The results showed that with this approach, a change in the psychophysiological state of the subject does not lead to a decrease in the accuracy of authentication. The best authentication error rates were: EER = 4.91 (FFR = 0.27 with FAR < 0.001). The proposed method is robust in relation to the user and his state, and is also efficient on small training samples (8 examples of thermograms per person).

Keywords: multilayer neural networks, biometrics to code neural network converters, automatic learning, facial thermograms, biometric authentication, feature extraction, feature informativeness estimation.

Bibliography — 25 references. *Received December 21, 2022*

УДК 004.056.53
DOI: 10.52190/2073-2600_2023_1_19
EDN: OKZLDQ

Конструирование модели обучающей нейронной сети для биометрической многофакторной аутентификации пользователя информационной системы

Р. Ф. Исмагилов; Н. Д. Лушников; А. С. Исмагилова, д-р физ.-мат. наук
ФГБОУ ВО «Уфимский университет науки и технологий», г. Уфа, Россия

Рассмотрен процесс программной реализации многофакторной биометрической аутентификации. Проанализированы нейросетевые методы распознавания человека. Рассмотрены особенности имитационного моделирования систем аутентификации личности по лицу человека. Разработан метод синтеза параметров математической модели сверточной нейронной сети, в которой обучающая выборка генерируется путем добавления искаженных образов посредством изменения рецептивных полей.

Ключевые слова: аутентификация, нейронная сеть, пользователь, информационная система, данные, безопасность, защита.

При автоматизированной обработке информации пользователь системы взаимодействует с вычислительными процессами устройства, которые выполняют операции с данными. Это создает риски неоднозначного сопоставления вычислительных процессов с тем или иным пользователем системы. Данные риски существуют и при автоматической обработке информации. Кроме того, удаленное информационное взаимодействие дополнительно порождает риск предоставления доступа злоумышленнику.

Аутентификация представляет собой действия по проверке подлинности пользователя системы, а также по проверке принадлежности пользователю системы предъявленного идентификатора доступа и аутентификационной информации [1].

Согласно приведенной терминологии, системе необходимо убедиться в подлинности предоставляемых пользователем системы данных. Для проверки подлинности используются форма авторизации (логин/пароль), модули распознавания личности по биометрическим образцам (лицо, голос, сетчатка глаза, отпечаток пальца и др.) [2].

Стоит обратить внимание, что в подавляющем большинстве рынок насыщен средствами двухфакторной биометрической идентификации. К числу основных подрядчиков по количеству проектов внедрений на рынке Российской Федерации в области информационной безопасности по направлению "Биометрическая идентификация" относятся такие крупные корпорации, как Банк Софт Системс (БСС) (охват рынка — 18,18 %), VisionLabs (6,06 %), Видеоматрикс (6,06 %). К числу зарекомендовавших себя ранее на международном рынке программных решений относятся Face ID (Apple Inc.), Luna Platform (VisionLabs) и Windows Hello (Microsoft). Данные технологии достигли высоких результатов в скорости обработки данных. Реализация процесса идентификации является удобной для пользователя учетной записи. Однако предоставляемый уровень защиты пользовательских данных еще не достиг требуемых показателей, необходимых потребителю.

Цель исследования — конструирование программного комплекса многофакторной биометрической аутентификации с использованием нейронных сетей и предоставление максимального уровня защиты информации пользователя любой информационной системы.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Изучить особенности распознавания личности по биометрическим образцам.
2. Изучить работу нейронных сетей.
3. Разработать программные модули многофакторной биометрической аутентификации пользователя информационной системы.
4. Создать обучающую нейронную сеть при обработке входных данных и определить ее конфигурацию.

Исмагилов Рузель Фанилевич, студент.
E-mail: ruzelismagilov@gmail.com
Лушников Никита Дмитриевич, аспирант.
E-mail: luschnikovnikita@yandex.ru
Исмагилова Альбина Сабирьяновна, профессор, зав. кафедрой.
E-mail: ismagilovaas@yandex.ru

Статья поступила в редакцию 20 декабря 2022 г.

5. Создать программный модуль шифрования биометрических образцов пользователя с использованием глубокого нейросетевого обучения.

Нормативно-правовое регулирование биометрической аутентификации

В нормативно-правовой части обозначен "Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы" (пункт I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ), Приказ ФСТЭК России от 11 февраля 2013 г. № 17), описываются термины и определения аутентификации, основы аутентификации, а также уровни доверия к результатам аутентификации (ГОСТ Р 58833-2020 "Защита информации. Идентификация и аутентификация"). Положения настоящего стандарта не исключают применение криптографических и биометрических методов (алгоритмов) при идентификации и аутентификации, но не устанавливают требования по их реализации [1].

К основным требованиям при разработке программного обеспечения относится создание логической структуры, в которой идентифицированы компоненты, их интерфейсы и концепция взаимодействия между ними (ГОСТ Р 56939-2016 "Защита информации. Разработка безопасного программного обеспечения").

Процессы аутентификации также косвенно взаимосвязаны с Федеральным законом "О персональных данных" от 27.07.2006 № 152-ФЗ. К информации, которая обрабатывается программным обеспечением, относятся в том числе и персональные данные пользователя системы. Для их легитимной обработки субъекту персональных данных (пользователю системы) необходимо подписать "Согласие на обработку персональных данных".

Реализация модулей программного комплекса

Для реализации многофакторной биометрической аутентификации и создания модели обучающей нейронной сети авторы использовали язык программирования Python (3.8 и 3.10). Выбор языка программирования обусловлен наличием необходимых библиотек (Tensorflow, OpenCV, IO, ffmpeg, dlib) для обработки информации (вывод онлайн-видеозаписи, доступ к микрофону и видеокамере, единовременное выполнение заданных программ) в синтезе с разработанными авторами элементами программной реализации модулей представленного комплекса. Язык программирования Python также удобен для интерпретации программных решений в виде мобильных приложений в тандеме с языком программирования Java (при установке библиотеки Node.js). К недостаткам выбранного языка программирования следует отнести отсутствие мультипликативности при программной реализации в другой операционной системе, а также высокие требования к производительной мощности устройства [3].

Обучающая и тестовая выборка нейронной сети

Для повышения уровня точности обработки данных создана нейронная сеть для обучения и сохранения результата нейронной сети в виде файла весов (формат .h5). Перед началом обучения необходимо собрать необходимые данные для распределения и дальнейшей классификации.

Структура нейронной сети состоит из трех папок, в том числе из папки "train", которая представляет собой обучающую выборку. DataSet был сформирован авторами самостоятельно и состоит из 300 обучающих биометрических образцов. Затем определяется количество эпох обучения, размер мини-выборки, заданное количество изображений для каждой папки.

Перед обучением указывается в процентном соотношении необходимое использование ресурсов устройства: центральный процессор и оперативная память. Так как количество классов в папках базы данных более двух, то компилирование модели обучающей нейронной сети реализуется с помощью категориальной кросс-энтропии по следующей формуле [4]:

$$L(p,t) = -\left[t\log_3(p) + (1-t)\log_3(1-p)\right], \qquad (1)$$

где t — ожидаемый результат обучения;
p — фактический результат обучения.

Стоит обратить внимание на то, что в обучении нейронной сетью будет задействовано 512 нейронов. Модель генерирует новую базу данных обработанных образцов, количество шагов в эпохах обучения, директорию сохраненных результатов обучения.

После окончания компиляции модели данные сверточной нейронной сети необходимо сгенерировать и представить в виде сохраненного файла весов обучающей нейронной сети. С помощью утилиты HDFView есть возможность наиболее подробно изучить поведение нейронов после пройденных итераций обработки данных.

С помощью данной утилиты также можно выбрать определенный набор данных и изменить его при необходимости. Данная функция предназна-

чена для реализации обучения нейронной сети по указанным настройками и параметрам.

При исходном выводе обучающей нейронной сети, равном $y_1, y_2, ..., y_n$, выход после процесса регрессии Softmax равен [5]:

$$\text{soft}\max\left(y_i\right) = y_i' = \frac{e^{y_i}}{\sum_{j=1}^{n} e^{y_i}}. \quad (2)$$

Соответственно:

$$\sum_{j=1}^{n} y_i' = 1. \quad (3)$$

Также в структуре нейронной сети присутствует папка "test", в которой сохранены результаты тестовой выборки. Объем DataSet тестового обучения составляет 300 биометрических образцов пользователя информационной системы.

Для программной реализации представленной структуры нейронной сети был применен принцип последовательного эксперимента, в котором размеры обучающей и тестовой выборок интенсивно увеличиваются до тех пор, пока не будет достигнут максимально высокий результат при обработке данных [6].

Оценка качества обучения нейронной сети

Для того, чтобы определить точность и качество работы обучающей нейронной сети, следует обратить внимание на функцию потерь с учетом всех погрешностей.

При помощи метода градиентного спуска с частной производной для подсчета функции ошибки используется следующая формула [7]:

$$\frac{\partial L}{\partial w_i} = \frac{\partial\left(y - y^*\right)}{\partial w_i} = 2\left(y - y^*\right)\frac{\partial\left(y - y^*\right)}{\partial w_i} = 2\left(y - y^*\right)\frac{\partial y}{\partial w_i}, \quad (4)$$

где w_i — i-й вес;

y — выход;

y^* — правильное значение выхода;

$\frac{\partial L}{\partial w_i} = \nabla L\left(\vec{w}\right)$ — градиент функции ошибки;

Δy — ошибка предсказания;

$f'\left(z\right)$ — значение производной функции f в точке $z = \sum_{i=1}^{n+1} x_i^* w_i$.

В процессе обучения вес увеличивается по формуле [8]:

$$\Delta w_i = -2\,\alpha\,\Delta y\; f'\left(z\right) x_i^*, \quad (5)$$

где w_i — i-й вес;

Δy — ошибка предсказания;

$\Delta y = y - y^*$ — величина ошибки предсказания;

α — коэффициент скорости обучения;

$f'\left(z\right)$ — значение производной функции f в точке $z = \sum_{i=1}^{n+1} x_i^* w_i$.

Стоит обратить внимание на изменение показателей обучающей нейронной сети (табл. 1).

Таблица 1

Значения второго слоя дискретизации после первой итерации

№	1	2	3
1	0,8264333	0,42032942	-0,6238235
2	-0,34823903	-1,6804181	-0,8202545
3	-0,66805077	-0,31023467	0.86219645

После действия 512 нейронов значения второго слоя дискретизации выглядят следующим образом (табл. 2).

Таблица 2

Значения второго слоя дискретизации после 512-й итерации

№	1	2	3
1	0,12990765	0,4991012	0,052575726
2	0,009280687	3,899197	-0,110825956
3	-0,037121985	-0,49370337	-0,027581342

Из представленных показателей глубокой нейронной сети следует, что уровень точности обучения имеет положительную динамику и расположенность к достижению максимальных показателей.

Оценка вычислительной сложности обучения нейронной сети

Корректная работа программного комплекса напрямую связана с вычислительной мощностью задействованного устройства. Для повышения качества и скорости обработки входных данных следует оценить вычислительную сложность обучения нейронной сети, подсчитав количество вычислительных операций. Общее количество вычислительных операций обучения нейронной сети

вычисляется по формуле нахождения величины одного порядка малости [9]:

$$S_{\text{кол.}} \approx \mathrm{O}\left(n^3 m\right) + \mathrm{O}\left(n^2 m\right) + \mathrm{O}\left(n^2 n_m\right) + \\ + \mathrm{O}\left(n^2 n_0\right) + \mathrm{O}\left(n n_m\right) + \mathrm{O}\left(n\right) + \mathrm{O}\left(n_m\right) \quad (6)$$

где $S_{\text{кол.}}$ — общее количество задействованных операций;

O — операция;

n — максимальное количество нейронов во всех скрытых слоях сети;

n_0 — количество входов сети;

n_m — количество выходов сети;

m — количество слоев в сети.

Из данного выражения очевидно, что вычислительная сложность зависит от количества нейронов в скрытых слоях. Однако стоит отметить, что для небольших значений показатель вычислительной сложности имеет низкий уровень.

Таким образом, обучающая нейронная сеть обладает большой вычислительной сложностью. Для достижения поставленной цели необходимо задействовать высокопроизводительные устройства.

Заключение

Представленные на рынке решения в области кибербезопасности не всегда соответствуют требуемым мерам защиты данных. Для предоставления максимального уровня защиты пользователя необходимо создать программный комплекс, который ограничит действия несанкционированного доступа злоумышленников. Для автоматизации программных модулей многофакторной аутентификации и повышения их точности при обработке данных необходимо использовать глубокие нейронные сети. К преимуществам использования обучающей нейронной сети следует отнести точность и качество обработки входных данных. Недостатками обучающей нейронной сети являются высокие требования к аппаратно-техническому комплексу и низкая скорость обработки данных.

Разработанный авторами программный комплекс представляет собой актуализированное решение на рынке кибербезопасности. Представленная модель сверточной нейронной сети в рамках программного комплекса является необходимым компонентом как при реализации распознавания личности по видео пользователя системы, так и при создании модуля шифрования данных пользователя.

Работа выполнена при финансовой поддержке гранта в форме субсидий в области науки из бюджета Республики Башкортостан для государственной поддержки молодых ученых.

Литература

1. ГОСТ Р 58833-2020 "Защита информации. Идентификация и аутентификация".

2. *Васильев В. И., Ложников П. С., Сулавко А. Е., Еременко А. В.* Технологии скрытой биометрической идентификации пользователей компьютерных систем // Вопросы защиты информации. 2015. № 3(138). С. 37—47.

3. *Лушников Н. Д., Исмагилова А. С.* Свидетельство о государственной регистрации программы для ЭВМ № 2021614672 Российская Федерация. Аутентификация учетных записей пользователей с помощью биометрических технологий: № 2021613387. Заявл. 15.03.2021. Опубл. 29.03.2021. Заявитель федеральное государственное бюджетное образовательное учреждение высшего образования "Башкирский государственный университет".

4. *Ван Лянпэн, Петросян О. Г.* Распознавание лиц на основе классификации вейвлет признаков путем вейвлет нейронных сетей // Информатизация образования и науки. 2018. № 4(40). С. 129—139.

5. *Хайкин С.* Нейронные сети. Полный курс. — М.: "Вильямс", 2006. — 1104 с.

6. *Лушников Н. Д., Исмагилова А. С.* Обучение и создание весов нейронной сети с применением категориальной кросс-энтропии: сб. мат. V Всеросс. молодежной науч.-практ. конф. "Информационные технологии обеспечения комплексной безопасности в цифровом обществе". Уфа, 20—21 мая 2022. С. 30—32. DOI: 10.33184/itokbco-2022-05-20.6.

7. *Гасников А. В.* Современные численные методы оптимизации. Метод универсального градиентного спуска: учеб. пособие. — М.: МФТИ, 2018. — 291 с.

8. *Гафаров Ф. М., Галимянов А. Ф.* Искусственные нейронные сети и приложения: учеб. пособие. — Казань: Изд-во Казан. ун-та, 2018. — 121 с.

9. *Fahlman Scott E., Lebiere Christian* "The Cascade-Correlation Learning Architecture" Advances in Neural Information Processing Systems 2, D.S. Touretzky, editor. Morgan Kaufmann 1990.

Designing a learning neural network model for biometric multifactor user authentication of an information system

R. F. Ismagilov, N. D. Lushnikov, A. S. Ismagilova
Ufa University of Science and Technology, Ufa, Russia

This article discusses the process of software implementation of multifactor biometric authentication. Neural network methods of human recognition are analyzed. The peculiarities of simulation modeling of face-based identity authentication systems are considered. The method of synthesis of parameters of mathematical model of convolutional neural network in which the training sample is generated by adding distorted images by changing the receptive fields is developed.

Keywords: authentication, neural network, user, information system, data, security, protection.

Bibliography — 9 references. *Received December 20, 2022*

УДК 004.056
DOI: 10.52190/2073-2600_2023_1_24
EDN: OLPSQM

Реализация принципов нулевого доверия при организации удалённого доступа в финансовых организациях

[1] *П. А. Иванов*, аспирант; [2, 3] *И. В. Капгер*, канд. техн. наук
[1] ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
[2] ФГБОУ ВО «Национальный исследовательский университет «МЭИ», Москва, Россия
[3] ФГБОУ ВО «Пермский национальный исследовательский политехнический университет», г. Пермь, Россия

Рассмотрены вопросы организации удалённого доступа к информационным системам финансовых организаций в соответствии с концепцией нулевого доверия на примере банковского сектора. Целью исследования является разработка комплексного подхода к организации удалённого доступа различных категорий пользователей к ресурсам финансовой организации, доступной из сети Интернет, который будет предоставлять достаточную степень защищённости информационных ресурсов в зависимости от их характера. Особенностью предложенного решения является архитектура удалённого доступа, построенная с соблюдением принципов нулевого доверия в сочетании с принципами классического подхода к построению информационной инфраструктуры.

Ключевые слова: информационная безопасность, нулевое доверие, удалённый доступ, информационные системы, финансовые организации.

Современные финансовые организации представляют собой сложные институты, которые в рамках своего функционирования перенимают множество качеств, характерных для ИТ-компаний, стремясь к повышению степени технологичности, применению инновационных технологий и решений, внедрению новых практик и созданию финансовых продуктов, которые предоставляются посредством информационных технологий.

Такие финансовые организации, как банки, фокусируются на развитии конкурентоспособных стратегий, что приводит к усложнению их организации, совмещению банковских и небанковских институтов, а также предоставлению ими услуг и выполнению операций, более типичных для ИТ-компаний, чем для финансовых организаций. В отличие от других отраслей, финансовая деятельность предполагает создание дистанционных сервисов и их предоставление для широкого круга лиц — клиентов, их партнеров и контрагентов, сотрудников, подрядчиков и т. п. Возникает необходимость проработки и реализации сложных схем удалённого доступа, которые должны быть созданы с учётом особенностей и потребностей каждой из групп пользователей этих сервисов, интересов и возможностей организаций и требований по информационной безопасности.

Целью статьи является разработка подхода к организации удалённого доступа пользователей различных категорий к информационной инфраструктуре организации, основанного на принципах нулевого доверия (Zero Trust Access, ZTA).

Данный подход должен обеспечивать реализацию удалённого доступа на нескольких условных "уровнях" — доступ клиентов и сотрудников организации, а также контрагентов организации. Поскольку каждая из групп пользователей имеет различную степень доверия и может привнести определённые риски, принципы нулевого доверия позволят достичь унифицированного решения, нивелирующего разницу для пользователей на каждом уровне.

Объектом рассмотрения является информационная инфраструктура финансовой организации, построенная по традиционной модели, в которой существует необходимость её адаптации к условиям удалённой работы сотрудников, а также для интеграции с облачными ресурсами и внешними сервисами. Необходимость адаптации следует отнести к ключевой особенности рассматриваемого объекта, поскольку большинство крупных финан-

Иванов Павел Алексеевич, аспирант Департамента информационной безопасности.
E-mail: 218666@edu.fa.ru
Капгер Игорь Владимирович, доцент кафедры "Безопасность и информационные технологии", доцент кафедры "Автоматика и телемеханика".
E-mail: Kapger@mail.ru

Статья поступила в редакцию 5 февраля 2023 г.

совых организаций не проектировали ИТ-инфраструктуры под нужды удалённых сотрудников и использование "облаков".

Принципы нулевого доверия [1], представленные Национальным институтом стандартов и технологий (NIST), появились в ответ на потребность государственных учреждений и частных компаний обеспечить безопасность своих разрастающихся информационных инфраструктур, которые за счёт внедрения новых, требующих совмещения с устаревшими и существующими, технологий и широкого распространения облачных вычислений, вынудили пересмотреть подход к их архитектуре [2]. За этим последовало появление новых продуктов от ведущих игроков рынка информационных технологий (VMware, Google, Palo Alto, Citrix, Microsoft и др.), учитывающих принципы нулевого доверия [3].

Под нулевым доверием следует понимать ряд принципов информационной безопасности, используемых при планировании и внедрении корпоративной информационной инфраструктуры, которые сфокусированы на конечных узлах, сервисах и потоках данных, а не на защищённом сетевом периметре [4]. Данную концепцию можно коротко охарактеризовать абстрактной моделью доступа (рис. 1), когда к любому ресурсу предприятия доступ из недоверенной зоны может быть предоставлен только через точки решения политики (policy decision point, PDP) и точку исполнения политики (policy enforcement point, PEP).

Существует множество подходов к интерпретации термина "нулевое доверие" и создании планов по переходу на подобную архитектуру, но все они основываются на базовых принципах, которые каждая организация применяет в соответствии со своими возможностями и потребностями [5]:

- отнесение данных, устройств или услуг к информационным ресурсам;
- отсутствие связи уровня доверия с местоположением сети и идентификацией ресурсов;
- предоставление доступа к отдельным ресурсам в рамках одной сессии доступа;
- определение доступа через динамические политики;
- отсутствие первоначального доверия к информационным активам;
- проведение постоянных проверок уровня доверия;
- строгий контроль процессов аутентификации и авторизации;
- сбор максимального количества информации об информационных активах.

Концепция нулевого доверия может быть реализована несколькими способами, которые основаны на базовых постулатах концепции, основными элементами которых являются расширенное управление идентификацией и аутентификацией, логическая и сетевая сегментация [1]. Построенная на этих постулатах архитектура будет иметь динамический характер и потребует периодического пересмотра и модернизации, который будет определяться изменениями в ИТ- и бизнес-потребностях.

Именно расширенная идентификация и аутентификация лежат в основе реализации управления и контроля удалённого доступа к ресурсам и сервисам организаций. Все конечные устройства — пользовательские автоматизированные рабочие места, портативные персональные компьютеры, мобильные устройства и т. д. являются потенциально недоверенными субъектами доступа, права которых не должны превышать минимально необходимых. Для субъектов, требующих более широких полномочий или административного доступа, подразумевается применение специализированных методов и инструментов обеспечения безопасности доступа таких субъектов.

Перед непосредственной разработкой подхода требуется анализ тех потребностей, которые существуют у финансовых организаций относительно пользовательского доступа. Первоочередной задачей является определение перечня субъектов доступа и условий предоставления доступа для каждого из них. Говоря о финансовых организациях, нельзя ограничиваться рассмотрением только пользователей-сотрудников — для них характерно наличие систем дистанционного обслуживания клиентов и контрагентов, причём зачастую — большого количества систем, отличающихся в плане организации доступа.

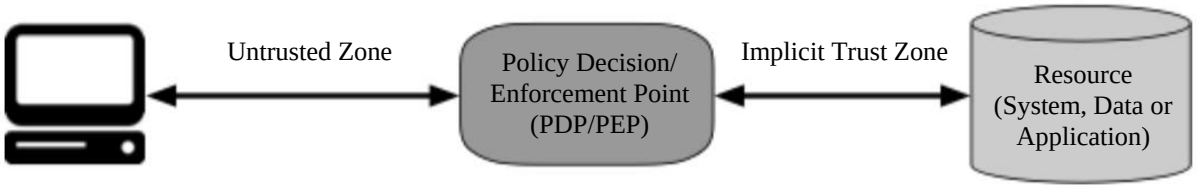


Рис. 1. Доступ с нулевым доверием (NIST SP 800-207 Zero Trust Architecture)

Следует выделить следующие основные типы субъектов доступа:

- клиенты организации,
- сотрудники организации,
- подрядчики и внешние разработчики,
- партнеры и контрагенты организации,
- государственные организации и регуляторы.

Первые три группы представляют собой классических пользователей информационных систем, которые используют существующие каналы пользовательского доступа и имеют различные потребности доступа (доступ к финансовым сервисам, таким, как системы дистанционного банковского обслуживания, системы контакт-центра и т. п., доступ к автоматизированным рабочим местам, доступ к средам разработки и тестовым контурам организации), а также различный уровень привилегий.

Оставшиеся группы являются более специфическими, поскольку требуют предоставления от финансовой организации каналов доступа к информационным сервисам, а также сервисам предоставления регуляторных сведений, включающих в себя и конфиденциальную информацию, причем часто к таким каналам предъявляют специфические требования, продиктованные как соблюдением законодательства в сфере защиты информации, так и спецификой информационных систем регуляторов.

Основной проблемой, которую необходимо решить, является гетерогенность каналов доступа для определённых типов субъектов. Доступ каждой из групп субъектов доступа не может быть реализован через единый механизм предоставления доступа и одного провайдера аутентификации, однако наиболее эффективным подходом является именно унификация механизмов доступа с учётом объективных трудностей реализации и технических ограничений.

Для упрощения процесса управления доступом следует использовать такой принцип концепции нулевого доверия, как отсутствие первоначального доверия к информационным активам (и субъектам доступа) — каждый запрос информационного актива изначально не может считаться доверенным. Сами субъекты доступа следует классифицировать не по уровню доверия к ним, что распространено в большой части организаций, а по применяемым к ним политикам доступа — для каждого типа субъектов доступа на стороне PDP применяется определённая совокупность статических и динамических политик, минимально достаточная для установления идентичности субъектов доступа и подтверждения доверия к ним в рамках каждого сеанса доступа к информационным активам.

С точки зрения архитектуры реализация такого подхода может быть разной, но стоит рассматривать создание единой точки доступа к активам, в рамках которой реализованы PDP и PEP для каждого типа субъектов доступа. Это дает преимущества для её контроля и мониторинга, а также упрощает маршрутизацию доступа к конечным защищённым активам. На рис. 2 представлена принципиальная модель предоставления удалённого доступа к инфраструктуре организации, которая условно разделена на следующие сегменты:

- доверенная зона — защищенные активы финансовой организации;
- зона безопасности, в рамках которой реализованы компоненты PDP и PEP;
- недоверенная зона — субъекты удалённого доступа, активы.

Доверенная зона, по сути, противоречит концепции ZTA, но её выделение диктуется гибридным характером рассматриваемого объекта исследования, поскольку ZTA встречается с традиционной концепцией защищённого периметра. В рамках модели вся доверенная зона является одним активом, а для активов в рамках доверенной зоны должны быть применимы все принципы нулевого доверия.

Зона безопасности — это ключевой элемент архитектуры удалённого доступа, который представляет собой выделенную инфраструктуру финансовой организации, на которой за счёт внедрения систем защиты информации (диагностики и мониторинга, соответствия стандартам, сводки об угрозах, инфраструктуры открытых ключей, управления доступом и других) реализуются компоненты PDP и PEP.

Недоверенная зона обозначает те активы, с которых устанавливаются сеансы доступа, т. е. устройства, используемые субъектами доступа. Следует рассматривать широкий перечь данных активов — персональные или корпоративные компьютеры, ноутбуки (в том числе защищённые ноутбуки, оборудованные соответствующим комплексом средств защиты информации), мобильные устройства (смартфоны и планшеты), терминалы (банкоматы, торговые терминалы и проч.), серверное оборудование и т. д. Фактически, это незащищённые и потенциально неизвестные устройства, доступ с которых может быть разрешен только после успешного прохождения проверок на основании определённых совокупностей политик доступа.

Рис. 2. Модель предоставления удаленного доступа к инфраструктуре финансовой организации

Все разрешительные политики доступа устанавливают и реализуют в рамках зоны безопасности, она является ключевым звеном в рамках реализации процессов управления доступа. Для каждого типа субъектов удалённого доступа предназначен так называемый домен зоны безопасности — часть общей инфраструктуры, в рамках которой располагаются соответствующие конкретным совокупностям политик доступа и реализующие их программно-аппаратные и программные средства.

Таким образом, основной задачей, которую требуется решить при создании зоны безопасности, является корректное определение необходимых политик, а также построение доменов с учётом особенностей субъектов доступа. В рамках принципиальной модели были выделены следующие домены, представленные в таблице.

Каждый домен должен быть построен таким образом, чтобы обеспечивался контроль выполнения политик при доступе со стороны различных субъектов. При этом необходимо заложить возможность внедрения специализированного программно-аппаратного и программного обеспечения, необходимость в котором может быть продиктована спецификой сервисов или реализующих их технологий — домены должны предусматривать использование нетиповых средств и по возможности снижать связанные с этим потенциальные риски нарушения политик безопасности.

Помимо этого, важным фактором обеспечения безопасности является сетевая и логическая микросегментация внутри доменов, поскольку каждый из них будет обеспечивать доступ к активам с различной степенью конфиденциальности и критичности для финансовой организации — права доступа, выданные в рамках одного из доменов, не должны давать возможности получить доступ к активам, контролируемых остальными доменами, а также повысить перечень прав доступа в рамках сессии доступа. Таким образом, верным будет утверждение, что субъект доступа может получить доступ только к тем активам, которые контролируются определённым доменом доступа и только в рамках сессии, открытой этим доменом.

Домены зоны безопасности модели предоставления удалённого доступа

Домен	Субъекты доступа	Основные задачи	Особенности
Предоставление удалённого доступа пользователей	Пользователи, привилегированные пользователи, подрядчики	Защищённый удалённый доступ, защищённый удалённый привилегированный доступ	Должен дублировать политики внутри доверенной зоны
Предоставление дистанционных сервисов	Клиенты	Доступ в неавторизованную зону, доступ в авторизованную зону	Должен разграничивать различные группы субъектов в зависимости от запрашиваемого сервиса
Предоставление технических сервисов	Партнеры, регуляторы	Доступ к публичным API, доступ к закрытым API, доступ к спец. сервисам	Должен обеспечивать политики для различных типов, подключаемых к нему активов

Преимуществом такого подхода будет более строгое разграничение доступа, позволяющее в большинстве случае исключить появление неправомерных сессий доступа, которые появляются в результате некорректной работы механизмов управления доступом. Каждому субъекту доступа потребуется подтверждать свою идентичность и правомерность своих прав путем обращения не к одной точке, а к нескольким, если это требуется. Так можно реализовать сложные ролевые модели для обеспечения безопасности совершенно разных активов фактически из одной точки, а также обеспечивать контроль и мониторинг таких доступов, проводить его аналитику в целях выявления недостатков в конфигурации PDP и PEP, путей их модернизации и совершенствования.

Литература

1. NIST Special Publication 800-207 Zero Trust Architecture, 59 pages (August 2020). DOI: doi.org/10.6028/NIST.SP.800-207.

2. *Garbis J., Chapman J. W.* Zero Trust Security: An Enterprise Guide; Springer: Berlin/Heidelberg, Germany, 2021.

3. *Sarkar S., Choudhary G., Shandilya S. K., Hussain A., Kim H.* Security of Zero Trust Networks in Cloud Computing: A Comparative Review // Sustainability. 2022. V. 14. P. 11213. https://doi.org/10.3390/ su141811213.

4. *Rose S, Borchert O, Connelly S, Mitchel S.* (2020) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg MD), NIST Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-207.

5. What Is Zero Trust Architecture? // [Электронный ресурс]: TrendMicro. URL: https://www.trendmicro.com/en_us/what-is/what-is-zero-trust/zero-trust-architecture.html (дата обращения: 18.06.2022).

Implementation of the principles of zero trust when organizing remote access in financial institutions

[1] *P. A. Ivanov,* [2, 3] *I. V. Kapger*

[1] Financial University under the Government of the Russian Federation, Moscow, Russia

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

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

The article describes the problems of remote access organization to information systems of financial organizations in accordance with the zero trust concept. The aim of this research is to develop a composite approach to remote access for various categories of users. The approach ensures a sufficient level of security to information resources depending on the category of users. A distinguishing feature of the proposed solution is a remote access architecture built in compliance with the zero trust principles and classical architectural approach of the protected perimeter.

Keywords: information security, zero trust, remote access, information systems, financial institutions.

Bibliography — 5 references.

Received February 5, 2023

УДК 003.26
DOI: 10.52190/2073-2600_2023_1_29
EDN: OMUFLQ

Способ сокращения размера подписи в рандомизированных алгоритмах ЭЦП

Е. В. Морозова, канд. техн. наук
Государственный университет морского и речного флота имени адмирала С. О. Макарова, Санкт-Петербург, Россия

А. А Костина
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН), Санкт-Петербург, Россия

Д. Н. Молдовян, канд. техн. наук
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Санкт-Петербург, Россия

Предложен способ уменьшения битовой длины подписи в рандомизированных алгоритмах ЭЦП двух разных типов, основанных на вычислительной трудности: задачи дискретного логарифмирования и решения систем многих квадратных уравнений с многими неизвестными. В рассмотренных алгоритмах ЭЦП рандомизирующий элемент подписи вычисляется как значение хэш-функции, поэтому для обеспечения L-битной стойкости к атакам на основе поиска коллизий требуется использовать хэш-функции с 2L-битными значениями. В предложенном способе используют две независимые хэш-функции с L-битными значениями. Одна из них служит для вычисления первого элемента подписи, а вторая — для вычисления значения хэш-функции h от подписываемого документа. Значение h входит в проверочное уравнение как степень при одном из множителей, что обеспечивает L-битный уровень стойкости к атакам на основе поиска коллизий при L-битном рандомизирующем элементе подписи.

Ключевые слова: компьютерная безопасность, цифровая подпись, постквантовая криптография, конечная ассоциативная алгебра, некоммутативная алгебра, скрытая группа, хэш-функция.

Всемирный конкурс по разработке постквантовых криптографических алгоритмов с открытым ключом, объявленный Национальным институтом стандартов и технологий США (НИСТ) в декабре 2016 г. на период 2017—2024 гг., перешел на завершающий четвертый этап [1]. В результате выполненных исследований в ходе первых трех этапов и подведения промежуточных итогов были выбраны три алгоритма электронной цифровой подписи (ЭЦП) CRYSTALS–Dilithium, FALCON, основанные на алгебраических решетках, и SPHINICS+, основанный на хэш-функциях, для стандартизации, и пять алгоритмов открытого согласования ключа для дальнейшего исследования. При этом НИСТ объявил дополнительный прием до 1 июня 2023 г. заявок на постквантовые алгоритмы ЭЦП, основанные на механизмах, отличных от тех, которые использованы в уже отобранных для стандартизации алгоритмах [2]. Этот факт показывает сохранение высокой степени актуальности задачи разработки практичных постквантовых алгоритмов ЭЦП, обладающих сравнительно малыми размерами подписи, открытого и секретного ключей.

Алгебраические алгоритмы ЭЦП со скрытой группой, основанные на вычислительной трудности решения системы многих квадратных уравнений с многими неизвестными [3—5], удовлетворяют последнему требованию. Эти алгоритмы относятся к типу рандомизированных схем ЭЦП, в которых первый элемент подписи e вычисляется как значение хэш-функции $f_H(M, R)$ от подписываемого документа M с присоединенным к нему значением фиксатора R.

Морозова Елена Владимировна, доцент.
E-mail: evmgumrf@mail.ru
Костина Анна Александровна, научный сотрудник.
E-mail: anya@hotbox.ru
Молдовян Дмитрий Николаевич, доцент.
E-mail: mdn.spectr@mail.ru

Статья поступила в редакцию 8 декабря 2022 г.

В данной работе предложен способ уменьшения размера рандомизирующего элемента подписи в два раза при сохранении уровня стойкости к атакам на основе поиска коллизий хэш-функции.

Реализация предлагаемого способа в алгоритме ЭЦП Шнорра

Алгоритм ЭЦП Шнорра [6] основан на вычислительной сложности задачи дискретного логарифмирования в простом конечном поле $GF(p)$, где $p = Nq + 1$ является простым числом большой разрядности. При этом число q является простым и его размер (битовая разрядность) задается, равным $2L$, при требовании обеспечения L-битного уровня стойкости (стойкости, равной 2^L операций модульного умножения). Открытый ключ формируется по формуле $y = \alpha^x \bmod p$, где x — секретный ключ; α — число, порядок которого по модулю p равен простому числу q.

Процедура генерации подписи к электронному документу M включает следующие шаги:

1. Подписант (являющийся владельцем открытого ключа y) генерирует случайное значение k (разовый секретный ключ), вычисляет значение фиксатора $R = \alpha^k \bmod p$ (разовый открытый ключ).

2. Используя некоторую специфицированную $2L$-битную хэш-функцию f_H, он вычисляет первый элемент подписи $e = f_H(M, R)$ в виде значения хэш-функции от документа с присоединенным к нему фиксатором.

3. Затем подписант вычисляет значение второго (подгоночного) элемента подписи $s = k + xE \bmod q$.

Подписью к электронному документу M является пара натуральных чисел (e, s). Верификация ЭЦП (проверка подлинности подписи) выполняется по следующей процедуре:

1. Вычислить значение $R' = y^{-e}\alpha^s \bmod p$.

2. Вычислить значение хэш-функции $e' = f_H(M, R')$.

3. Сравнить значения e' и e. Если $e' = \ddot{e}$, то подпись признается подлинной, иначе — ложной.

Существуют два типа существенно различных атак с вычислением значения хэш-функции. К первому типу относят атаки подделки подписи, когда фальсификатор пытается сгенерировать правильное значение подписи (т. е. подпись, проходящую проверочную процедуру как подлинная подпись) без знания секретного ключа, т. е. значения x. Для этого фальсификатор генерирует случайные пары значений (ε, σ). Для каждой перебираемой пары он вычисляет значения $\rho = y^{-\varepsilon}\alpha^\sigma \bmod p$ и $\varepsilon' = f_H(M, \rho)$, после чего проверяет выполнимость равенства $\varepsilon' = \varepsilon$. Легко видеть, что для $2L$-битной хэш-функции вероятность выполнения последнего равенства равна 2^{-2L}, а значит, количество указанных вычислительных попыток, которые должен выполнить фальсификатор для подделки подписи к документу, примерно равно $2^{2L}/2 = 2^{2L-1}$, т. е. вычислительная сложность этой атаки имеет порядок $O(2^{2L})$ операций вычисления хэш-функции, где $O(\bullet)$ — обозначение порядка значения, указанного в скобках. Вычисление секретного значения x по открытому ключу с использованием хорошо известного ρ-метода Полларда для решения задачи дискретного логарифмирования требует выполнения существенно меньшего числа операций, а именно, выполнения $O(q^{1/2}) \approx O(2^L)$ операций умножения по модулю p. Это означает, что последний вариант атаки первого типа является более эффективным.

Ко второму типу атаки относят атаки, в которых осуществляется поиск двух различных документов M и M', для которых значения $f_H(M)$ и $f_H(M')$ равны. При этом в силу итеративности процесса вычисления значения хэш-функции для произвольного значения R будет выполняться равенство $f_H(M, R) = f_H(M', R)$. Если один из документов представить подписанту, например, M на подпись, и он сформирует к нему подпись, то эта подпись будет подлинной и для документа M'. Таким образом, получаем сценарий атаки, известный как "атака с помощью секретарши", включающая подмену документа M, подписанного начальником, на документ M', который направляется секретаршей тому или иному адресату.

Вычислительная сложность поиска коллизии для $2L$-битной хэш-функции, не имеющей слабостей (их наличие уменьшает эту сложность), равна $O(2^L)$. Поскольку стойкость алгоритма ЭЦП определяется атакой с наименьшей вычислительной сложностью, то для получения L-битного уровня стойкости алгоритма Шнорра следует использовать $2L$-битную хэш-функцию. Поскольку первый элемент подписи (e, s) вычисляется как значение хэш-функции, то его разрядность будет составлять $2L$ бит. Такой же размер имеет и второй элемент подписи, поскольку он вычисляется, как остаток от деления некоторого значения на $2L$-битное простое число q. Таким образом, при требовании обеспечения L-битного уровня стойкости размер подписи в алгоритме Шнорра равен $4L$ бит (или более).

Идея способа сокращения размера подписи состоит в том, чтобы вместо одной $2L$-битной хэш-функции f_H использовать две независимые L-битные хэш-функции f_1 и f_2. При этом одну хэш-

функцию f_1 предполагается использовать для вычисления хэш-значения от документа M: $h = f_H(M)$, а вторую — для вычисления первого элемента подписи $e = f_H(M, R)$, причем дополнительное хэш-значение h предполагается включить в проверочное уравнение, например, следующим образом:

$$R' = y^{-e}\alpha^{sh} \bmod p.$$

Легко видеть, что возможны и другие варианты использования значения в проверочном уравнении, например, $R' = y^{-e+h}\alpha^{sh} \bmod p$ или $R' = y^{-e/h}\alpha^{sh} \bmod p$. Принципиальным является задание зависимости степеней в правой части проверочного уравнения от L-битных значений e и h.

Такое модифицирование приводит к уменьшению разрядности первого элемента подписи в два раза, т. е. до значения L бит. При этом вычислительная сложность первого варианта подделки подписи, основанного на поиске совпадения значений ε' и ε, уменьшается до значения $O(2^L)$ операций вычисления хэш-значения, но не нарушает L-битного уровня стойкости.

Вычислительная сложность атаки, основанной на поиске коллизий хэш-функций, после модифицирования не изменяется, поскольку теперь потребуется найти общую коллизию для двух L-битных хэш-функций f_1 и f_2, что имеет такую же вычислительную сложность, как и поиск коллизии одной $2L$-битной хэш-функции f_H (действительно, вычисление двух значений независимых хэш-функций от одного и того же входного значения можно рассмотреть, как единую своеобразную $2L$-битную хэш-функцию f_{12}).

Таким образом, предложенный способ модифицирования алгоритма Шнорра позволил уменьшить размер подписи с начальных $4L$ бит до $3L$ бит при сохранении L-битного уровня стойкости.

В следующих разделах рассмотрим применение описанного способа уменьшения размера подписи по отношению к постквантовым алгебраическим алгоритмам ЭЦП со скрытой группой, стойкость которых основана на вычислительной трудности решения системы многих квадратных уравнений с многими неизвестными [5, 7]. В этих алгоритмах в качестве алгебраического носителя используются конечные некоммутативные ассоциативные алгебры (КНАА), заданные над простым полем $GF(p)$. Элементами КНАА являются векторы m-мерного векторного пространства, координаты которых являются элементами поля $GF(p)$. Фактически m-мерная КНАА представляет собой m-мерное векторное пространство, в котором задана дополнительная операция — умножение векторов, обладающее свойствами замкнутости, дистрибутивности слева и справа относительно операции сложения, некоммутативности и ассоциативности. Способы задания операции умножения для КНАА различных размерностей и типов описаны в работах [8—10]. Далее используем обозначения векторов большими латинскими буквами, представленными прямым полужирным шрифтом.

Реализация способа в алгоритмах ЭЦП со скрытой группой

1. Случай проверочного уравнения с тремя вхождениями подписи

В схеме ЭЦП [7], в которой в качестве алгебраического носителя используется шестимерная КНАА, заданная над простым конечным полем $GF(p)$ при простом 96-битном числе q, открытый ключ формируется следующим образом.

Задается случайная скрытая группа путем генерации двух случайных обратимых векторов **G** и **H** порядка q, являющихся элементами секретного ключа и образующих ее базис <**G**, **H**>. Для этого необходимо выполнить следующие действия:

1. Выбрать случайный вектор **V**, порядок которого равен $p - 1$ и который не входит в подмножество скалярных векторов.
2. Вычислить вектор $\mathbf{G} = \mathbf{V}^2$.
3. Выбрать случайное натуральное число k $(0 < k < p - 1)$ и случайный примитивный элемент $\beta \in GF(p)$.
4. Выполняя скалярное умножение на β^2, вычислить вектор $\mathbf{H} = \beta^2\mathbf{G}^k$.

Затем выполняя следующие шаги, формируется секретный ключ:

1. Выбрать случайные обратимые векторы **A**, **B**, и **D**, для которых выполняются неравенства $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AD} \neq \mathbf{DA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{DB} \neq \mathbf{BD}$, $\mathbf{BG} \neq \mathbf{GB}$, $\mathbf{DG} \neq \mathbf{GD}$.
2. Вычислить обратные векторы $\mathbf{A}^{-1}$, $\mathbf{B}^{-1}$ и $\mathbf{D}^{-1}$.
3. Выбрать случайные натуральные числа x и w $(x < q; w < q)$.

Секретным ключом является пятерка векторов **A**, **B**, **D**, **G**, и **H** и пара чисел x и w. Размер секретного ключа составляет примерно 355 байт.

Открытый ключ (**Y**, **Z**, **U**, **V**) размером 258 байт вычисляется по формулам:

$$\mathbf{Y} = \mathbf{B}^{-1}\mathbf{G}\mathbf{A}^{-1};\ \mathbf{Z} = \mathbf{B}^{-1}\mathbf{H}\mathbf{A}^{-1};\ \mathbf{U} = \mathbf{B}^{-1}\mathbf{G}^x\mathbf{D}^{-1};$$
$$\mathbf{V} = \mathbf{D}\mathbf{H}^w\mathbf{A}^{-1}.$$

Процедура генерации ЭЦП, осуществляется по следующему алгоритму:

1. Выбрать случайные натуральные числа $k < q$ и $t < q$ и вычислить вектор

$$\mathbf{R} = \mathbf{D}\,\mathbf{G}^k\mathbf{H}^t\,\mathbf{D}^{-1}.$$

2. Используя некоторую 384-битную хэш-функцию хэш-функции f_H, вычислить первый (рандомизирующий) элемент ЭЦП e в виде конкатенация трех 128-битных натуральных значений e_1, e_2 и e_3: $e = e_1||e_2||e_3$ = хэш-функции $f_H(M, \mathbf{R})$, где M — подписываемый документ.

3. Вычислить натуральные значения n и u по следующим двум формулам:

$$n = \frac{k - e_1e_2e_3 - xe_3}{e_1e_2e_3 + e_2e_3 + e_3} \bmod q;$$

$$u = \frac{t - e_2e_3 - we_3}{e_1e_2e_3 + e_2e_3 + e_3} \bmod q.$$

4. Вычислить вектор **S**, представляющий собой подгоночный элемент ЭЦП:

$$\mathbf{S} = \mathbf{A}\mathbf{G}^n\mathbf{H}^u\mathbf{B}. \quad (9)$$

Подпись представляет собой пару (e, **S**), т. е. хэш-значение e и вектор **S**. Длина подписи равна ≈113 байт.

Проверка подлинности ЭЦП к документу M выполняется по открытому ключу (**Y**, **Z**, **U**, **V**) в соответствии со следующей процедурой.

Алгоритм верификации ЭЦП.

1. Вычислить вектор-фиксатор

$$\mathbf{R}' = \left[\mathbf{V}\left(\mathbf{S}(\mathbf{YS})^{e_1}\mathbf{Z}\right)^{e_2}\mathbf{SU}\right]^{e_3}.$$

2. Вычислить хэш-значение e' = хэш-функции $f_H(M, \mathbf{R}')$.

3. При выполнении равенства $e' = e$ подпись признается подлинной, иначе она отвергается как ложная.

В рассмотренном алгоритме 144-битный уровень стойкости к атакам второго типа определяется размером значения первого элемента подписи $e = e_1||e_2||e_3$, который равен 288 бит. Легко видеть, что для реализации предлагаемого способа сокращения размера подписи следует использовать две 144-битные хэш-функции f_1 и f_2 и задать вычисление дополнительного хэш-значения h по формуле $h = h_1||h_2 = f_1(M)$, где h_1 — 96-битное число и h_2 — 48-битное число. При этом первый элемент подписи следует вычислить по формуле $e = e_1||e_2 = f_2(M, \mathbf{R})$, где e_1 — 96-битное число и e_2 — 48-битное число, а вычисление вектора-фиксатора на первом шаге процедуры верификации ЭЦП задать по формуле

$$\mathbf{R}' = \left[\mathbf{V}\left(\mathbf{S}(\mathbf{YS})^{e_1}\mathbf{Z}\right)^{h_1}\mathbf{SU}\right]^{e_2h_2}.$$

Такая модификация проверочного уравнения требует изменения формул, по которым на шаге 3 процедуры генерации ЭЦП выполняется вычисление степеней n и u, используемых для вычисления подгоночного элемента подписи **S**. Легко показать, что корректность работы модифицированной схемы ЭЦП обеспечивают следующие формулы:

$$n = \frac{k - e_1e_2h_1h_2 - xe_2h_2}{e_1e_2h_1h_2 + e_2h_1h_2 + e_2h_2} \bmod q;$$

$$u = \frac{t - e_2h_1h_2 - we_2h_2}{e_1e_2h_1h_2 + e_2h_1h_2 + e_2h_2} \bmod q.$$

В модифицированной схеме ЭЦП размер первого элемента подписи в два раза меньше, чем в исходной схеме, и составляет 18 байт. Это определяет сокращенный размер подписи (e, **S**), равный ≈95 байт.

2. Случай проверочного уравнения с четырьмя вхождениями подписи

В алгоритме ЭЦП [5] с проверочным уравнением с четырьмя вхождениями подписи в качестве алгебраического носителя используется четырехмерная КНАА, заданная над полем $GF(p)$ с характеристикой $p = 2q + 1$, где q — простое 160-битное число. В качестве секретного ключа используется набор из четырех векторов **A**, **B**, **G**, и **H** и натурального числа x ($1 < x < q$), причем векторы **G** и **H** имеют порядок, равный q, и составляют базис <**G**, **H**> скрытой группы. Векторы **A** и **B** являются случайными и обратимыми и удовлетворяют неравенствам $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{BG} \neq \mathbf{GB}$.

Открытый ключ формируется как тройка векторов **Y**, **Z** и **U** следующим образом:

$$\mathbf{Y} = \mathbf{AGB}, \mathbf{Z} = \mathbf{AG}^x\mathbf{B} \text{ и } \mathbf{U} = \mathbf{AHB}.$$

Процедура генерации подписи к электронному документу M включает следующие шаги:

1. Выбрать случайные натуральные числа k и t($k < q$; $t < q$) и вычислить вектор-фиксатор

$$\mathbf{R} = \mathbf{B}^{-1}\mathbf{G}^k\mathbf{H}^t\mathbf{B}.$$

2. Используя специфицированную 320-битную хэш-функцию f_H, вычислить первый элемент подписи $e = e_1||e_2 = f_H(M||\mathbf{R})$, где$e_1$ и e_2 являются 160-битнымичислами.

3. Вычислить степени n и d по следующим формулам:

$$n = \frac{k - e_1 - e_1^2 - xe_1}{e_1(e_1 + e_2 + 1)} \bmod q;$$

$$d = \frac{t - e_1e_2}{e_1(e_1 + e_2 + 1)} \bmod q.$$

4. Вычислить вектор **S** (подгоночный элемент подписи) по формуле

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{A}^{-1}.$$

Подпись (*e*, **S**) имеет размер ≈121 байт. Проверка подлинности ЭЦП включает следующие вычислительные шаги:

1. Вычислить вектор **R′** по формуле

$$\mathbf{R}' = \left((\mathbf{SY})^{e_1} \mathbf{S} (\mathbf{US})^{e_2} \mathbf{ZSY} \right)^{e_1}.$$

2. Вычислить значение хэш-функции $e' = f_H(M||\mathbf{R}')$.

3. При выполнении равенства $e' = e$ подпись признается подлинной, иначе ($e' \neq e$) — ложной.

Этот алгоритм ЭЦП обладает 160-битной стойкостью к атакам второго типа, что определяется использованием 320-битной хэш-функцией для вычисления первого элемента подписи $e = e_1||e_2$. В соответствии с предложенным способом, сокращение размера подписи достигается использованием двух 160-битных хэш-функций f_1 и f_2. Хэш-функция f_2 используется для вычисления 160-битного рандомизирующего элемента подписи: $e = f_2(M||\mathbf{R})$, а хэш-функция f_1 — для вычисления дополнительного 160-битного хэш-значения $h = f_1(M)$, которое следует внести в проверочное уравнение, что можно сделать модифицированием этого уравнения, задавая его в следующем виде:

$$\mathbf{R}' = \left((\mathbf{SY})^{e} \mathbf{S} (\mathbf{US})^{h} \mathbf{ZSY} \right)^{e}.$$

В алгоритме ЭЦП с проверочным уравнением последнего вида на шаге 3 процедуры генерации ЭЦП вычисление степеней *n* и *d*, используемых для вычисления подгоночного элемента подписи **S**, следует выполнить по формулам:

$$n = \frac{k - e - e^2 - xe}{e(e + h + 1)} \bmod q;$$

$$d = \frac{t - eh}{e(e + h + 1)} \bmod q.$$

Производительность процедур генерации и верификации в модифицированной схеме ЭЦП практически не изменяется, а размер первого элемента подписи сокращается в два раза и становится равным 20 байт. При этом размер сокращенной подписи (*e*, **S**)равен ≈101 байт.

Обсуждение

Предложенный способ сокращения размера подписи может быть применен также и к другим известным постквантовым алгебраическим алгоритмам ЭЦП, основанным на вычислительной трудности решения системы многих квадратных уравнений, например, рассматриваемым в работах [11,12]. При этом уровень стойкости модифицируемого алгоритма не изменяется. Вычисление двух разных хэш-значений (один раз только от документа, а второй раз — от документа с присоединенным фиксатором) уменьшает производительность алгоритма. Однако этот недостаток можно устранить следующим путем.

Дополнительное хэш-значение *h* можно вычислять с использованием хэш-функции f_H, используемой в исходном алгоритме, а затем брать остаток от деления полученного значения $f_H(M)$ на простое число *r*, разрядность которого равна половине разрядности хэш-функции f_H, т. е. по формуле $h = f_H(M) \bmod r$. Затем, используя сохраненное значение $f_H(M)$, вычислить рандомизирующий элемент подписи по формуле

$$e = f_2\left(f_H(M), \mathbf{R} \right),$$

где разрядность хэш-функции f_2 в два раза меньше разрядности f_H. Благодаря тому, что хэш-значение $f_H(M)$ уже вычислено на предыдущем шаге, аргумент хэш-функции f_2 имеет достаточно малый размер, поэтому нахождение ее значения не будет вносить существенной задержки в процедуры генерации и верификации ЭЦП, практически сохраняя исходное значение производительности алгоритма ЭЦП.

Действительно, алгоритмы хэширования строятся в виде итеративной процедуры — аргумент (входное сообщение) разбивается на блоки данных одинакового размера, и выполняется многократное вычисление значения раундовой хэш-функции в зависимости от текущего блока данных и от предыдущего значения раундовой хэш-функции. Следовательно, во сколько раз уменьшится размер входного сообщения, во столько раз уменьшится время вычисления значения хэш-функции.

Можно предложить и другие формулы для быстрого вычисления рандомизирующего элемента подписи, например, $e = Rf_H(M) \bmod r_2$, где *R* — натуральное число, представляющее собой конкатенацию всех координат вектора **R**, r_2 — простое число, имеющие разрядность, равную разрядности числа *r*, причем числа r_2 и *r* выбираются случайным образом.

Заключение

Рассмотренный способ сокращения размера подписи в рандомизированных алгоритмах ЭЦП представляет практический интерес, поскольку он не уменьшает производительности исходного модифицируемого алгоритма. В частности, способ может быть применен для сокращения размера подписи в алгебраических схемах ЭЦП, основанных на скрытой задаче дискретного логарифмирования [13, 14].

Литература

1. *Alagic G., Apon D., Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J. Yi-Kai Liu, Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D.* Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NIST IR 8413, National lnstitute of Standards and Technology, July 2022. — 99 p. [Электронный ресурс]. Режим доступа: https://doi.org/10.6028/NIST.IR.8413 (дата обращения: 01.12.2022).
2. Call for Additional Digital Signature Schemes forthe Post-Quantum Cryptography Standardization Process. September 6, 2022. — 99 p. [Электронный ресурс]. Режим доступа: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf (дата обращения: 01.12.2022).
3. *Молдовян Д. Н., Молдовян А. А., Молдовян Н. А*. Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах // Вопросы кибербезопасности. 2022. № 1(47). С. 18—25.
DOI: 10.21681/2311-3456-2022-1-18-25.
4. *Курышева А. А., Костина А. А., Молдовян Н. А.* Алгебраические алгоритмы со скрытой группой над конечными полями характеристики два // Вопросы защиты информации. 2022. № 2. С. 13—20. DOI: 10.52190/2073-2600_2022_2_13.
5. *Молдовян Д. Н.* Типовые проверочные уравнения в алгебраических алгоритмах ЭЦП со скрытой группой // Вопросы защиты информации. 2022. № 1. С. 31—37.
DOI: 10.52190/2073-2600_2022_1_31.
6. *Молдовян Д. Н., Молдовян А. А.* Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // Вопросы кибербезопасности. 2022. № 2(48). С. 7—17. DOI: 10.21681/2311-3456-2022-2-7-17.
7. *Schnorr C. P.* Efficient signature generation by smart cards // J. Cryptology. 1991. V. 4. P. 161—174.
8. *Moldovyan D. N., Moldovyan N. A.* A post-quantum digital signature scheme on groups with four-dimensional cyclicity // Информационно-управляющие системы. 2021. № 2. С. 43—51. DOI: 10.31799/1684-8853-2021-2-43-51.
9. *Молдовян А. А., Молдовян Д. Н., Молдовян Н. А., Костина А. А.* Конечные кватернионоподобные алгебры как носители постквантвых алгоритмов ЭЦП // Вопросы защиты информации. 2022. № 2. С. 21—29.
DOI: 10.52190/2073-2600_2022_2_21.
10. *Молдовян Д. Н.* Задание шестимерных алгебр как носителей криптосхем, основанных на скрытой задаче дискретного логарифмирования // Вопросы защиты информации. 2021. № 1. С. 26—32. DOI: 10.52190/2073-2600_2021_1_26.
11. *Moldovyan A. A., Moldovyan D. N.* A New Method for Developing Signature Algorithms. Bulletin of Academy of Sciences of Moldova. Mathematics, 2022. № 1(98). P. 56—65.
DOI: https://doi.org/10.56415/basm.y2022.i1.p56.
12. *Молдовян А. А., Молдовян Н. А.* Алгоритмы ЭЦП на конечных некоммутативных алгебрах над полями характеристики два // Вопросы кибербезопасности. 2022. № 3(49). С. 58—68. DOI: 10.21681/2311-3456-2022-3-58-68.
13. *Moldovyan D. N.* A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. V. 29. № 2(86). P. 206—226.
14. *Moldovyan N. A., Moldovyan A. A.* Digital signature scheme on the 2x2 matrix algebra // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2021. Т. 17. Вып. 3. С. 254—261.

A method for reducing the signature size in randomized algorithms

E. V. Morozova
Admiral Makarov State University of Maritime and Inland Shipping, St. Petersburg, Russia

A. A. Kostina
St. Petersburg Federal Research Center of the RAS (SPC RAS), St. Petersburg, Russia

D. N. Moldovyan
St. Petersburg Electrotechnical Univeristy "LETI", St. Petersburg, Russia

A method is proposed for reducing the bit length of the signature in randomized digital signature algorithms of two different types, based on the computational difficulty: of the discrete logarithm problem and of solving systems of many quadratic equations with many unknowns. In the considered signature algorithms, the randomizing element of the signature is calculated as a hash function value, therefore, in order to provide L-bit resistance to attacks based on collision search, it is required to use hash functions with $2L$-bit values. The proposed method uses two independent hash functions with L-bit values. One of them is used to calculate the first element of the signature, and the second one is used to calculate the value of the hash function h from the signed document. The value of h enters the check equation as a power at one of the factors, which provides an L-bit level of resistance to attacks based on collision search with an L-bit randomizing signature element.

Keywords: computer security, digital signature, post-quantum cryptography, finite associative algebra, non-commutative algebra, hidden group, hash-function.

Bibliography — 14 references. *Received December 8, 2022*

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004.056
DOI: 10.52190/2073-2600_2023_1_35
EDN: PDEMTW

Пользовательские и персональные данные: анализ рисков "извлечения знаний"

П. Г. Былевский, канд. филос. наук
Институт информационных наук МГЛУ (МГПИИЯ им. М. Тореза), Москва, Россия
Финансовый университет при Правительстве РФ, Москва, Россия

В статье анализируются риски автоматизированного анализа больших пользовательских данных, связанные с возможностями несанкционированного получения конфиденциальной информации. Приоритет обработки больших данных у операторов-генераторов, в том числе нерезидентов России. Обезличивание/деидентификация данных как мера безопасности противоречит их содержательной ценности для интеллектуальной аналитики. Решить проблему предлагается регулированием посредством общей, отраслевых и локальных моделей критических идентификаторов больших данных.

Ключевые слова: большие данные, пользовательские данные, риски, извлечение знаний, автоматический анализ, безопасность

Цель данной работы — исследование возможностей и рисков автоматизированного анализа пользовательских данных, актуализированных в 2022 г. в связи с обострением реконфигурации международных отношений, снижением безопасности и фрагментацией глобального киберпространства. Пользовательские данные, подпадая под законодательное определение персональных, ещё меньше защищены государством, хотя значительно превосходят их по критичности (содержательности, образованию больших данных и связанностью с конфиденциальными сведениями). Также пользовательские данные посредством автоматизированного анализа консолидированных баз данных могут быть использованы, чтобы идентифицировать граждан на основе технических данных и наоборот, персонализировать технические данные.

Интеллектуальная автоматическая аналитика больших пользовательских данных допускает возможность выделения конфиденциальной статистики и критической информации вплоть до высоких уровней секретности, порождая риски не только для граждан, их общностей и коммерции, но и для национальной безопасности. Хотя указанные возможности соотносимы с разведкой из открытых источников, но значительно более содержательны, тем не менее, доступ государства к большим пользовательским данным ограничен в сравнении с корпоративными операторами и покупателями. Просматриваются риски не только несанкционированного доступа, но и злоупотреблений со стороны операторов, в особенности не резидентов, глобальных информационных платформ, базирующихся за рубежом, в недружественных странах.

Рассмотрим решение данной проблемы в следующей последовательности: представление методологии исследования; анализ возможностей получения конфиденциальной информации посредством анализа больших пользовательских данных; рассмотрение несоответствия анонимизации/деидентификации и содержательной ценности итогов автоматической аналитики, доказательство необходимости отраслевых и локальных моделей критических идентификаторов. Заключительные выводы содержат предлагаемые меры обработки указанных рисков, которые могут быть полезными для совершенствования государственного регулирования обеспечения безопасности больших пользовательских данных и людей.

Былевский Павел Геннадиевич, доцент кафедры международной информационной безопасности, доцент департамента информационной безопасности.
E-mail: pr-911@yandex.ru

Статья поступила в редакцию 24 декабря 2022 г.

Актуальные риски больших пользовательских данных

Нормативное регулирование, профессиональное и научное обсуждение безопасности больших пользовательских данных сосредоточено на аспектах предотвращения технических угроз непрерывности их обработки и несанкционированного доступа (извне или утечек). Просматривается унификация подхода ко всем видам больших данных как техническим, так и персональным в широком смысле (включая данные пользовательские и данные о людях) [1]. Специфика персональных данных учитывается лишь в отношении их "узкого" перечня (защищаемого Роскомнадзором), не учитываются в должной мере риски реализации данных пользовательских и о людях как персональных. Но здесь осуществляется защита лишь прав граждан как субъектов персональных данных.

Однако содержательные возможности познания посредством автоматизированной аналитики больших данных, в том числе пользовательских и о людях, намного более значительны, порождая сопутствующие риски иных типов и более высокого уровня. Таким риском, скорее имеющим отношение к конкурентной политике, чем к информационной безопасности, является неравенство возможностей в области торговли ими их операторами. Именно в таком виде встал вопрос о нормативном регулировании больших пользовательских данных в России ещё в 2017 г. [2]. В 2018 г. была создана отраслевая саморегулируемая организация "Ассоциация больших данных", включающая участников этого рынка, в том числе "Яндекс", VK, "МегаФон", "Сбербанк" и др. организации.

Наряду с созданием отраслевого сообщества в Государственной Думе РФ был разработан законопроект № 571124-7 "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" [3] — законодательная инициатива в области больших пользовательских данных. Законопроект формулировал понятия этих данных (как "совокупности, не содержащей персональных данных информации о физических лицах и (или) их поведении, не позволяющая без использования дополнительной информации и (или) дополнительной обработки определить конкретное физическое лицо, собираемой из различных источников, в том числе сети Интернет, количество которых превышает тысячу сетевых адресов"), их операторов и их обязанностей.

Участники рынка отраслевого бизнес-сообщества стремились обработать риски коммерческого характера. Законодательная инициатива была направлена главным образом на защиту прав граждан как субъектов пользовательских данных, которые могут быть использованы для их идентификации. Тем самым на данные пользовательские и о людях проецировался тот же методологический подход, что и в защите персональных данных, предусмотренной ФЗ-152 и осуществляемой Роскомнадзором.

Признавались риски нарушения прав на тайну, неприкосновенность личной жизни, связанные с данными пользовательскими и о гражданах, однако не учитывался существенно более высокий уровень угроз из-за их намного большей содержательности в сравнении с "обычными" персональными данными. На основе целевой консолидации баз разных видов больших персональных данных (пользовательских и о людях) потенциально возможно подробное непрерывное отслеживание граждан в режиме реального времени [4], а посредством автоматизированного анализа — распознавание и прогнозирование предпочтений, действий, настроений и эмоций, мыслей и поступков.

Прогнозируемые риски больших пользовательских данных

Повышенные риски нарушения индивидуальных прав граждан на основе содержательной аналитики больших пользовательских данных не были учтены в законопроекте № 571124-7. Но это не единственные риски, сопутствующие большим пользовательским данным [5]. Заслуживают внимания, изучения и обсуждения возможности получения таким путём не только детализированных подробных сведений об отдельных гражданах в режиме реального времени [6]. Консолидация различных видов больших пользовательских данных различных операторов (социальных сетей, операторов мобильной связи и интернет-провайдеров, торговых и финансовых организаций и т. д.) создаёт почти безграничные возможности для аналитики, в том числе предиктивной [7], на основе их автоматизированной статистики.

Конфиденциальная информация, которая может быть несанкционированно получена [8] на основе анализа больших пользовательских данных, не сводится к подробностям в реальном времени неприкосновенной личной жизни отдельных граждан [9]. Подобные же сведения могут стать доступными и в отношении *разного масштаба групп, сообществ и общностей граждан* [10], включая всех граждан государства, соотносимо с вопросами *национальной безопасности*. В результате автоматизированного анализа больших пользовательских данных могут быть получены и ста-

тистические данные, подпадающие под определение конфиденциальной информации (возможно, вплоть до относящихся к государственной тайне).

Большие пользовательские данные генерируются, передаются, обрабатываются и хранятся их операторами, которым открыты широкие возможности непосредственной автоматизированной статистики собственных баз и приобретаемых на партнёрской или коммерческой основе [11]. Напротив, возможности доступа государственных органов к корпоративным базам больших персональных данных и их обновлениям в режиме реального времени являются ограниченными действующим законодательством, другими нормативно-правовыми документами, сформулированными в них процедурами. В частности, представители государства, уполномоченные вести оперативно-розыскную деятельность, ограничены в доступе к корпоративным базам больших пользовательских данных сильнее, чем сотрудники их операторов.

Риски несанкционированного получения конфиденциальной информации посредством автоматизированного анализа операторами больших персональных данных возрастают в связи с тем, что среди них есть глобальные информационные корпорации, работающие на территории России, в отечественном киберпространстве и с российскими гражданами. Следует учитывать, что в условиях реконфигурации международных отношений, снижением безопасности и фрагментацией глобального киберпространства самые крупные и влиятельные из этих информационных платформ являются резидентами США и других недружественных стран. Даже в условиях ограничений на трансграничную передачу больших пользовательских данных остаются такие возможности в отношении результатов их анализа собранных больших пользовательских данных, способных содержать несанкционированно полученную конфиденциальную информацию.

Минимизация рисков безопасности итогов автоматической аналитики

Мерой безопасности персональных данных является анонимизация (обезличивание) со встречными рисками деанонимизации (реперсоналиции) посредством автоматического анализа с использованием косвенных идентификаторов, консолидации дополнительных баз данных и моделирования исходного контекста [12]. В отношении пользовательских данных также может быть применено понятие анонимизации (обезличивания) и риски деанонимизации (персонализации). Однако анализу пользовательских данных присущи риски не только персонализации и извлечения конфиденциальных знаний об отдельных гражданах, но также и о группах и сообществах [13], а также знаний, соотносящихся с закрытой информацией об объектах и процессах, в том числе критической инфраструктуры. Отсюда в отношении автоматического анализа больших данных пользовательских и о людях могут применяться требования как анонимизации, так и деидентификации критических содержательных параметров, соотносимых с оборудованием, программным обеспечением, объектами и процессами среды.

В отношении больших данных пользовательских, о людях и технических (намного более содержательных, подробных и детализированных) аналогичной мерой безопасности является деидентификация параметров. Перечень удаляемых (деидентифицируемых) параметров должен формироваться на основе оценки рисков получения на их основе автоматическим анализом конфиденциальной информации. Возвращаясь к аналогии с "добычей" и "обогащением" "сырых данных", здесь уместно понятие "обеднения руды". Причём "обогащение" по одним параметрам может выборочно проводиться наряду с "обеднением" по другим [14].

Риски несанкционированного получения конфиденциальной информации посредством автоматического анализа больших данных пользовательских, о людях и технических могут относиться не только к гражданам, но и к объектам и процессам, в том числе критической инфраструктуры. В первую очередь — это риски операторов-генераторов, ибо идентификаторы, имеющие отношение к конфиденциальной информации, могут находиться в "сырых" больших данных. Риски могут реализоваться непосредственно для операторов-генераторов в случае получения ими конфиденциальной информации автоматизированным анализом.

По-видимому, невозможно полностью устранить риски автоматизированного "извлечения знаний" конфиденциального характера непосредственными операторами больших данных (персональных, пользовательских, о людях и технических) иначе, как посредством ограничений самой возможности генерации данных, анализ которых может привести к получению конфиденциальной информации. Для минимизации указных рисков операторы-генераторы, осуществляющие автоматических анализ больших данных, должны оценивать результаты на предмет отсутствия конфиденциальной информации.

Мера "деидентификации" больших данных и риски их "реидентификации" (по аналогии с ано-

нимизацией и деанонимизацией персональных данных) относится к рискам передачи этих данных контрагентам (в том числе продажи, партнёрства, не считая несанкционированного доступа). Несанкционированное получение конфиденциальной информации операторами-контрагентами посредством автоматического анализа деидентифицированных больших данных может включать моделирование исходного контекста, использование косвенных идентификаторов и консолидированных баз данных.

Определение критических идентификаторов для больших данных

Риски получения конфиденциальной информации автоматической статистики могут транслироваться на контрагентов в случае передачи (продажи) им баз больших данных. В частности, в тех случаях, когда передачу не предваряет целевая деидентификация, или при некорректном "обеднении" (удалении критичных идентификаторов). Обязанность "деидентифицировать" параметры больших данных, соотносимые с конфиденциальной информацией, могут быть возложены на их операторов-генераторов для случаев передачи (продажи) таких баз данных контрагентам.

Понизить риски извлечения конфиденциальной информации автоматической обработкой консолидированных для передачи больших данных операторами-генераторами вовне можно требованиями деидентифицировать большие данные (анонимизировать персональные) [15]. Это требует составления перечня критических параметров-идентификаторов на основе предварительной сформированной моделей угроз, в том числе отраслевых, региональных и для организаций. Универсальный перечень критических идентификаторов больших данных может иметь лишь самый общий характер [16]. Для отраслей, регионов, разных периодов времени, конкретных объектов и процессов востребованы специализированные перечни таких критических идентификаторов.

Как это часто бывает, интересы безопасности передачи (партнёрства, продажи) больших данных приходят в противоречие с бизнес-интересами. Деидентификация (деанонимизация) больших данных снижает их содержательность, возможности получения нужной автоматизированной статистики, поэтому может быть лишь частичной, неполной. Однако сохранение после целевой частичной деидентификации части идентифицирующих (содержательных) параметров, способных иметь критическое значение, снижает риски автоматизированного "извлечения знаний" конфиденциального характера, но не может устранить их полностью. Повышение уровня деидентификации (анонимизации) больших данных в указанных целях соответственно снижает их ценность для покупателей.

Формулировка требований к деидентификации (деанонимизации) больших данных должна соотноситься, с одной стороны, с рисками получения конфиденциальных сведений автоматическим анализом, с другой стороны, — с соответствующими изменениями их коммерческой ценности. Недостатки прогнозирования рисков и модели угроз могут привести к недостаточной деидентификации (деанонимизации), включая сохранение неучтённых критических параметров (идентификаторов) данных [17]. Решением может служить требование к операторам-генераторам продавать (передавать) контрагентам не "сырые" (пусть даже обезличенные, анонимизированные) большие данные, а только результаты автоматической статистики, осуществляемой по техническому заданию заказчика, с предварительной проверкой отсутствия в них конфиденциальной информации.

Следует признать безосновательно преувеличенным обсуждение темы "утечек баз персональных данных", риски которых несоизмеримо малы в сравнении с потенциальными опасностями злоупотреблений автоматизированной аналитикой больших пользовательских данных их операторами. Проанализированные риски заслуживают изучения и дальнейшего анализа, включая создание моделей угроз несанкционированного доступа к разным видам конфиденциальной информации посредством автоматизированного анализа больших персональных данных. Такая работа может помочь классифицировать и ранжировать указанные риски, что необходимо для выработки и осуществления эффективных мер безопасности.

Заключение

Исследование потенциальных возможностей познания объектов и процессов (извлечения знаний) посредством автоматизированного анализа больших пользовательских данных выявляет ряд пока мало учитываемых рисков.

Большие пользовательские данные при консолидации дополнительных подобных баз разных типов и применении автоматизированных инструментов анализа могут деанонимизироваться и реализовываться как персональные данные. Таким образом, возникают риски таргетированного (целевого) нарушения конфиденциальности, несанкционированного доступа к данным о личной жизни (в том числе о поведении, предпочтениях,

эмоциях, мыслях и т. п.) вплоть до непрерывного в режиме реального времени. Подобные риски могут возникать в отношении как граждан, так и их общностей, вплоть до вопросов национальной безопасности.

Автоматизированный анализ консолидированных больших пользовательских данных позволяет на основе данных пользовательских и о людях "персонализировать" технические данные и в качестве выводов несанкционированно получать статистические сведения, могущие подпадать под определения конфиденциальной информации разного уровня секретности.

Приоритет возможностей автоматизированного анализа больших пользовательских данных принадлежит, с момента их генерации, частным коммерческим первичным операторам и покупателям (в том числе резидентам не России, а недружественных стран). Доступ государственных организаций, кроме тех случаев, когда они сами выступают операторами больших пользовательских данных, вторичен и ограничен законодательством и другими нормативными актами, предписанными ими процедурами.

Большие пользовательские данные могут быть отнесены к критически важным, в таком случае оптимально их государственное регулирование, наподобие объектов ограниченного оборота (оружия, средств стойкой криптографии, сильнодействующих психотропных веществ и т. п.).

Анализ этих существующих, потенциальных и прогнозируемых рисков позволяет сделать выводы о необходимости проведения исследований (определение понятия, классификация категорий, выработка моделей угроз и т. д.), обсуждения и выработки мер безопасности посредством государственного и общественного регулирования больших данных пользовательских и о людях.

Литература

1. *Романова А. Ю.* К вопросу о правовом режиме больших данных // Конституционное и муниципальное право. 2019. № 8. С. 20—25.

2. Глава Роскомнадзора считает необходимым скорейшую выработку норм регулирования в области больших пользовательских данных. 9 ноября 2017 года [Электронный ресурс]. Режим доступа: https://rkn.gov.ru/news/rsoc/news51776.htm (дата обращения: 18.12.2022).

3. О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации". Законопроект № 571124-7 [Электронный ресурс]. Режим доступа: https://sozd.duma.gov.ru/bill/571124-7 (дата доступа: 18.12 2022).

4. *Сычев Н. В., Жорин Ф. В., Андряков Д. А., Бадрутдинов А. Д.* Обзор негласных средств слежения в мобильных устройствах // Спецтехника и связь. 2014. № 1. С. 14—16.

5. *Кобышев К. С., Монастырев В. В., Никифоров И. В., Ткачев И. П., Сердюков А. Д.* Автоматизированная система для анализа пользовательских данных и их классификации по социальным группам с общими интересами: мат. науч. конф. с международным участием "Неделя науки СПбПУ". Санкт-Петербург, 19–23 ноября 2019. С. 73—76.

6. *Mrabet H., Belguith S., Alhomoud A., Jemai A.* A survey of IoT security based on a layered architecture of sensing and data analysis // Sensors. 2020. № 20(13). P. 3625. DOI: 10.3390/s20133625.

7. *Федорова А. А., Терехов В. И.* Применение предиктивной аналитики на основе пользовательских данных в платежной банковской системе: тезисы докладов XVIII Всеросс. науч. конф. "Нейрокомпьютеры и их применение". Москва, 17 марта 2020. С. 75—76.

8. *Корниенко С. В.* Big Data: проблемы безопасности пользовательских данных // Академия педагогических идей новация. Серия: студенческий научный вестник. 2019. № 2. С. 48—52.

9. *Вульфин А. М.* Интеллектуальный анализ данных пользовательского окружения в задаче обнаружения удаленного управления // Моделирование, оптимизация и информационные технологии. 2020. Т. 8. № 2(29). С. 1—19. DOI: 10.26102/2310-6018/2020.29.2.011.

10. *Rudikowa L., Myslivec O., Sobolevsky S., Nenko A., Savenkov I.* The development of a data collection and analysis system based on social network users' data // Procedia Computer Science. V. 156. P. 194—203.

11. *Зыонг К. Х. Т., Кравец А. Г.* Анализ API-доступа к социальным сетям для сбора пользовательских данных // Инновационные, информационные и коммуникационные технологии. 2019. № 1. С. 391—394.

12. *Мищенко Е. Ю., Соколов А. Н.* Определение эффективности обезличивания персональных данных с использованием модели нарушителя // Вестник УРФО. Безопасность в информационной сфере. 2020. № 2(36). С. 34—42.

13. *Шведова В. О.* Цифровые идентификаторы личности как новый источник социальной дискриминации // Социальная интеграция и развитие этнокультур в евразийском пространстве. 2020. Т. 3. № 9. С. 239—244.

14. *Jiang Y., Yang G., Li H., Zhang T.* Knowledge driven approach for smart bridge maintenance using big data mining // Automation in Construction. 2023. V. 146. — 21 p. https://doi.org/10.1016/j.autcon.2022.104673

15. *Спеваков А. Г., Калуцкий И. В.* Устройство формирования уникальной последовательности, используемой при обезличивании персональных данных // Труды МАИ. 2020. № 115. — 25 с. DOI: 10.34759/trd-2020-115-13.

16. *Wei G., Shao J., Xiang Y., Zhu P., Lu R.* Obtain confidentiality or/and authenticity in Big Data by ID-based generalized signcryption // Information Sciences. 2015. V. 318. P. 111—122.

17. *Narayanan U., Paul V., Joseph S.* A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment // J. King Saud University — Computer and Information Sciences. 2022. V. 34. № 6. Part B. P. 3121—3135.

User and personal data: risk analysis of "knowledge extraction"

P. G. Bylevsky
Institute of Information Sciences of MGLU (MGPIII named after M. Torez), Moscow, Russia
Financial University under the Government of the Russian Federation, Moscow, Russia

The article analyzes the risks of automated analysis of large user data associated with the possibility of unauthorized receipt of confidential information. The priority of big data processing for generator operators, including non-residents of Russia. Depersonalization/deidentification of data as a security measure contradicts their meaningful value for intellectual analytics. It is proposed to solve the problem by regulation through general, industry and local models of critical identifiers of big data.

Keywords: big data, user data, risks, knowledge extraction, automatic analysis, security.

Bibliography — 17 references. *Received December 20, 2022*

УДК 004.056.5
DOI: 10.52190/2073-2600_2023_1_41
EDN: PWUHZJ

Обоснование инструментально-расчетного метода оценки информационных потерь в цифровых приемных устройствах технических средств разведки

А. В. Душкин, д-р техн. наук; *Ю. В. Савченко*, д-р техн. наук
Национальный исследовательский университет «Московский институт электронной техники», г. Зеленоград, Москва, Россия

В. А. Щербаков, д-р техн. наук; *И. С. Рекунков*, канд. техн. наук
Военная академия РВСН им. Петра Великого, г. Балашиха, Московская обл., Россия

Приводятся результаты обоснования инструментально-расчетного метода оценки информационных потерь в приемных устройствах цифровых средств разведки на основе процедур измерения плотностей распределения вероятностей мгновенных значений полезных сигналов и помех на входе приемника. Обоснованы вероятностные критерии информационных потерь и предложены процедуры их количественной оценки на входе и выходе приемника с помощью современной измерительной аппаратуры. Дан пример применения информационного критерия в практике испытаний приемного устройства на помехозащищенность.

Ключевые слова: помехозащищенность, информационные потери, технические средства разведки.

В задачах испытаний приемников современных цифровых устройств инфокоммуникационных систем на эффективность и помехозащищенность актуальным научным направлением является совершенствование методов количественной оценки потерь информации, обусловленных воздействием радиопомех различного вида на приемники технических средств разведки. Наиболее полно эти методы проработаны в монографии [1], в которой обоснована инфологическая модель информационного конфликта радиосредств в спектре электромагнитных волн. В рамках этой модели авторами монографии предложен новый показатель в виде относительных информационных потерь на выходе цифровых линий радиосвязи при конфликте со средствами радиоэлектронного подавления. Этот новый показатель отличается от известных энергетических показателей помехозащищенности и эффективности радиоэлектронного подавления (защитное отношение, коэффициент подавления) учетом влияния видов и параметров законов распределений мгновенных значений амплитуд сигналов и помех на рабочее отношение помеха—сигнал. Учет законов распределения амплитуд сигналов и помех позволяет более адекватно оценивать как помехозащищенность приемных устройств средств связи, так и эффективность средств радиоэлектронного подавления в динамике информационного конфликта между цифровыми линиями передачи информации и средствами создания организованных и непреднамеренных помех [2].

В упомянутой монографии [1] аналитическим способом и путем моделирования получены соотношения помеха—сигнал для типовых законов распределения сигналов и помех на входе приемника (для логарифмически-нормального и гамма-распределений). Вместе с тем, как показывает опыт испытания цифровых средств связи на эффективность и помехозащищенность, в условиях реальной эксплуатации радиосредств законы распределений мгновенных значений сигналов и помех могут отличаться от теоретически обоснованных законов. В таких ситуациях снижается качество моделей, приведенных в [1], с практической точки зрения.

Исходя из этого, целью данной статьи является обоснование практически реализуемого с помощью современной цифровой измерительной техники метода количественной оценки относитель-

Душкин Александр Викторович, профессор кафедры.
E-mail: a_dushkin1@mail.ru
Савченко Юрий Васильевич, профессор кафедры.
E-mail: a_dushkin1@mail.ru
Щербаков Виталий Алексеевич, заместитель начальника кафедры.
E-mail: svasvarog@yandex.ru
Рекунков Иван Сергеевич, докторант кафедры.
E-mail: ivan.grek.1982@mail.ru

Статья поступила в редакцию 14 февраля 2023 г.

ных информационных потерь на входе и выходе цифровых радиоприемных устройств для оценки влияния вида и параметров помех на качество приема цифровых каналов связи.

Поставленная цель достигается обоснованием информационного показателя помехозащищенности, а также метода его количественной оценки инструментальным способом при испытаниях цифровых радиосредств на эффективность и помехозащищенность.

Обоснование информационного показателя помехозащищенности

В работах [3—7] предложен информационно-энтропийный подход для количественной оценки качества радиопомех и помехозащищенности радиоприемных устройств, сущность которого заключается в определении различия статистических характеристик флюктуаций амплитуды сигналов и помех, а именно количественной меры близости плотностей распределения вероятностей (ПРВ) мгновенных значений сигналов и помех (либо их аддитивной смеси). Примем этот подход за основу при обосновании универсального информационного показателя помехозащищенности, определяемого экспериментально.

Закон распределения мгновенных значений (или огибающей) амплитуд флуктуирующих сигналов и помех имеет жесткую функциональную связь с энергетическим спектром сигнала или помехи, поэтому показатель помехозащищенности приемника можно представить в виде

$$h(A) = \frac{p_n(A)}{p_s(A)}, \qquad (1)$$

где $p_n(A)$ — плотность распределения вероятностей мгновенных значений амплитуд помехи;

$p_s(A)$ — плотность распределения вероятностей мгновенных значений амплитуд полезного цифрового сигнала.

Измерительные технологии определения законов распределений мгновенных амплитуд сигналов и помех в настоящее время находят все более широкое применение в практике испытаний радиосредств на радиоэлектронную защиту [7].

Изменение энергетического спектра сигнала (помехи) приводит к изменению формы закона распределения мгновенных значений их амплитуд, поэтому на практике в (1) вместо ПРВ мгновенных значений амплитуд используют характеристику формы закона распределения, а именно — энтропию ПРВ. Энтропия ПРВ является интегральной числовой моментной характеристикой закона распределения и в случае стационарного характера случайного процесса полностью характеризует вероятностные свойства сигналов и помех. С учетом отмеченного, интегральный вероятностный энтропийный показатель (1) можно переписать в виде

$$h_i(A) = \frac{H_n(A)}{H_s(A)}, \qquad (2)$$

где $H_n(A) = -\int p_n(A) \ln p_n(A) dA$ — энтропия плотности распределения вероятностей мгновенных значений амплитуд помехи, измеренная на входе приемника;

$H_s(A) = -\int p_s(A) \ln p_s(A) dA$ — энтропия плотности распределения вероятностей мгновенных значений амплитуд полезного сигнала, измеренная на входе приемника.

Поскольку энтропия ПРВ — это интегральный показатель, учитывающий через форму закона распределения вероятностные свойства амплитудного спектра сигнала (помехи), то введенный показатель (2) является более общим по сравнению с показателем (1). Новый информационно-энтропийный показатель (2) является дальнейшим развитием не только известного энергетического показателя защитного отношения, но и предложенного в работе [1] показателя относительных информационных потерь при воздействии радиопомех на цифровые каналы связи. Главным отличием данного показателя от известных показателей является возможность его простой количественной оценки экспериментальным способом с помощью серийно выпускаемой аппаратуры по инженерной методике. При этом энтропия ПРВ сигнала и энтропия ПРВ помехи измеряются на входе исследуемого цифрового приемника поочередно при подаче на приемник полезного сигнала и помехи с известными параметрами.

Необходимо отметить, что при расчете показателя (1) необходимо выполнять математическую операцию деления функции на функцию, а при расчете показателя (2) — деления числа на число.

В практических задачах оценки качества заградительных устройств по частоте шумов и помех вместо энтропии ПРВ целесообразно применять традиционно используемый показатель — коэффициент качества шума, который также измеряют и рассчитывают путем цифровой обработки мгновенных значений напряжений электрического сигнала шума или помехи. Коэффициент качества

шума определяют через энтропию ПРВ по формуле

$$\eta(A)=\frac{\exp\{H(A)\}}{\sqrt{2\pi e\sigma^2}}, \qquad (3)$$

где σ — среднеквадратическое отклонение мгновенных значений исследуемого сигнала от его математического ожидания.

С учетом (3) следующий вариант информационно-энтропийного показателя по аналогии с (2) можно записать в виде

$$\delta\eta(A)=\frac{\eta_n(A)}{\eta_s(A)}. \qquad (4)$$

Таким образом, показатели вида (1), (2), и (4) являются вероятностными информационно-энтропийными и обеспечивают количественную оценку эффектов от воздействия преднамеренных и непреднамеренных радиопомех с любыми законами распределения мгновенных значений в практически важных приложениях испытаний аппаратуры цифровых каналов связи на эффективность, помехозащищенность и помехоустойчивость. Их применение существенно повышает достоверность и качество методического аппарата для оценки эффективности средств и комплексов радиосвязи.

Метод количественной оценки относительных информационных потерь

Изложим сущность метода количественной оценки относительных информационных потерь в виде просто поддающейся алгоритмизации последовательности измерительных процедур по получению численных значений показателей (1), (2) и (4). На первом этапе оценки функционального показателя вида (1) необходимо определить статистические характеристики мгновенных значений помехи (шума). В основу технологии определения указанных характеристик положим методический подход, разработанный в патенте на изобретение [7].

Реализации шума или помехи в виде электрического сигнала шума или помехи записывают в оперативной памяти измерительного приемника (например, векторного анализатора спектра) в течение заданного интервала времени, а затем подвергают операции дискретизации во времени с требуемым шагом дискретизации. На следующем этапе обработки записанного массива информации для всех дискретных моментов времени $t_j(j=\overline{1,M})$ измеряют уровни напряжений электрического сигнала помехи или шума, выбирают среди всех измеренных значений максимальный $u_{\max}$ и минимальный $u_{\min}$ уровни напряжения помехи (шума) и разбивают весь диапазон измеренных значений указанных напряжений на N уровней. Напряжение u_i каждого i-го уровня вычисляют по формуле

$$u_i=\left(i-\frac{N}{2}\right)\Delta u, \qquad (5)$$

где $i=\overline{1,N}$ — номер уровня напряжения исследуемого сигнала шума или помехи;

N — количество уровней напряжения исследуемого электрического сигнала;

$$\Delta u=\frac{u_{\max}-u_{\min}}{N}.$$

После выполнения математических операций (5) в течение интервала времени t вычисляют количество N_i пересечений электрическим сигналом каждого i-го уровня и рассчитывают общее количество пересечений s-м электрическим сигналом всех уровней по формуле

$$S=\sum_{i=1}^{N}N_i. \qquad (6)$$

На следующем этапе алгоритмической статистической обработки электрического сигнала помехи или шума рассчитывают вероятности p_i пересечения каждого i-го уровня по формуле

$$p_i=\frac{N_i}{S}. \qquad (7)$$

По результатам измерений вероятностей (7) строят гистограмму закона распределений мгновенных значений исследуемого сигнального процесса $p_i(u_i),(i=\overline{1,N})$. После построения гистограммы вычисляют средневзвешенное значение (оценку математического ожидания) u_m обрабатываемого массива мгновенных значений электрического сигнала шума или помехи на интервале $[u_{\min}, u_{\max}]$ по формуле

$$u_m=\sum_{i=1}^{N}u_i p_i. \qquad (8)$$

Далее рассчитывают среднеквадратическое отклонение напряжения электрического сигнала шума (помехи) по формуле

$$\sigma=\sqrt{\sum_{i=1}^{N}(u_i-u_m)^2\,p_i}. \qquad (9)$$

На заключительных этапах алгоритмизированной процедуры определения энтропийно-информационного показателя потерь информации за счет влияния помех и шумов вычисляют следующие параметры:

- энтропию $H_N(u)$ плотности распределения вероятностей мгновенных значений напряжения электрического сигнала помехи или шума по формуле

$$H_n(u) = -\sum_{i=1}^{N} p_i \ln p_i , \qquad (10)$$

- энтропийный коэффициент качества шума $\eta(u)$ с любым законом распределения мгновенных значений напряжения

$$\eta(u) = \frac{\exp\{H_n(u)\}}{\sqrt{2\pi e\sigma^2}}. \qquad (11)$$

Измерительные процедуры (5)—(11) повторяют при подаче вместо шума или помехи полезного сигнала на вход приемника, т. е. определяют параметры $H_s(u), \eta_s(u)$. Таким образом, измерительную процедуру определения информационно-энтропийных показателей помехозащищенности приемника или качества помех выполняют последовательно в два этапа. На первом этапе на вход исследуемого цифрового приемника подают помеху заданного вида, а на втором этапе — типовой (тестовый) полезный информационный цифровой сигнал от другого радиосредства (корреспондента) или имитатора сигналов.

Завершается практическая реализация определения относительных информационных потерь в соответствии с новой предложенной технологией нахождения частного от деления в соответствии с формулами

$$h(u) = \frac{p_n(u)}{p_s(u)};\ h_i(u) = \frac{H_n(u)}{H_s(u)};\ \delta h(u) = \frac{\eta_n(u)}{\eta_s(u)}. \qquad (12)$$

Все указанные процедуры метода количественной оценки показателей (1), (2) и (4), а именно соотношения (5)—(12) достаточно просто реализуются путем программирования интерфейсных приложений к современным цифровым измерительным приборам (векторным анализаторам спектра и анализаторам цепей). В аналоговом виде измерение энтропии ПРВ мгновенных значений амплитуд сигналов и помех может быть реализовано с помощью серийно выпускаемых и метрологически-аттестованных приборов ряда Х1 (измерителей статистических характеристик сигналов).

Необходимо отметить, что все известные методики ориентированы на измерение энтропии ПРВ только на входе измерительного прибора или исследуемого цифрового приемника. Вместе с тем, известно, что при прохождении сигналов и помех по нелинейным цепям вид закона распределения их мгновенных значений существенно изменяется. Наличие в приемнике узлов с нелинейными электрическими свойствами (например, усилителей с нелинейной вольтамперной характеристикой) приводит к изменению значений оцениваемых показателей (1), (2) и (4) на выходе приемника по сравнению с соответствующими значениями на входе приемника. При детальных исследованиях влияния трактов приемников на значение относительных информационных потерь возникает задача учета влияния нелинейностей тракта приема на качество приема в условиях помех. С экспериментальной точки зрения эта задача является трудоемкой и требует последовательного выполнения экспериментов по оценке информационных потерь как на входе, так и на выходе приемника. Для сокращения трудоемкости измерений целесообразно применить следующую измерительно-расчетную процедуру.

Оценка относительных информационных потерь на выходе цифрового приемного устройства

Сущность упрощенной практически реализуемой методики оценки относительных информационных потерь на выходе цифрового приемного устройства заключается в следующем. Последовательность действий по достижению требуемого результата включает следующие операции:

- измеряют передаточную характеристику тракта приемника по напряжению $K_0(U) = \left(U_{off} / U_{on}\right)$ при фиксированной частотной настройке приемника;
- измеряют ПРВ мгновенных значений напряжений сигналов и (или) помех на входе цифрового приемника $p_n(u), p_s(u)$;
- путем перемножения параметра $K_0(U)$ на ПРВ $p_n(u)$ или $p_s(u)$ получают измененный закон распределения мгновенных значений напряжений сигналов (помех) на выходе приемника:

$$p_{noff} = K_0(u)\, p_n(u); \quad p_{soff} = K_0(u)\, p_s(u),$$

- по формулам (1), (2), (4) определяют значение искомого показателя относительных информационных потерь на выходе приемного устройства или на выходе участка приемного тракта с нелинейными электрическими свойствами (при

расчете (1) выполняется математическая операция умножения функции на число);

- все указанные процедуры повторяют для другой частотной настройки приемника.

В заключение приведем некоторые фрагменты результатов исследования относительных информационных потерь на входе цифрового приемника радиостанции, выполненные путем программирования (опции) цифрового анализатора спектра Agilent MXA N9020 A. На вход приемника радиостанции подавали полезный сигнал с нормальным законом распределения амплитуд и сигнал помехи с логарифмически-нормальным законом распределения мгновенных амплитуд. Данные о значениях входных статистических параметров сигнала и помехи приведены на рис. 1. Результат оценки показателя (1), полученный в соответствии с предложенным инструментально-расчетным методом оценки относительных информационных потерь при воздействии радиопомех на цифровые радиоприемные устройства, приведен на рис. 2. При получении результата для наглядного представления результирующей функции (1) применен алгоритм, заимствованный из источника [7].

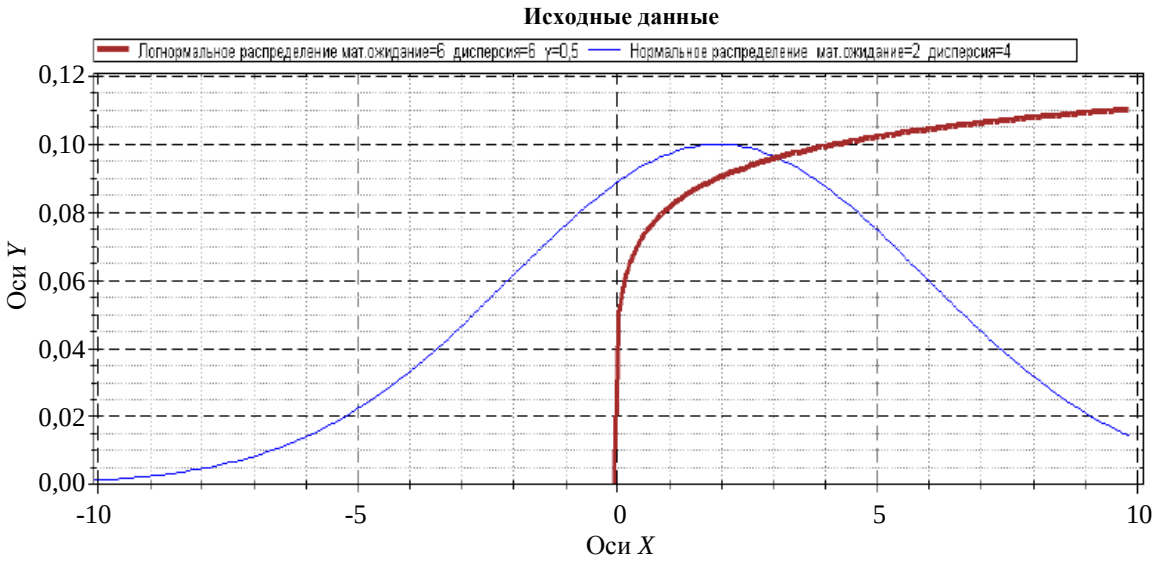


Рис. 1. Плотности вероятностей распределения мгновенных значений амплитуд сигнала и помехи на входе анализатора спектра

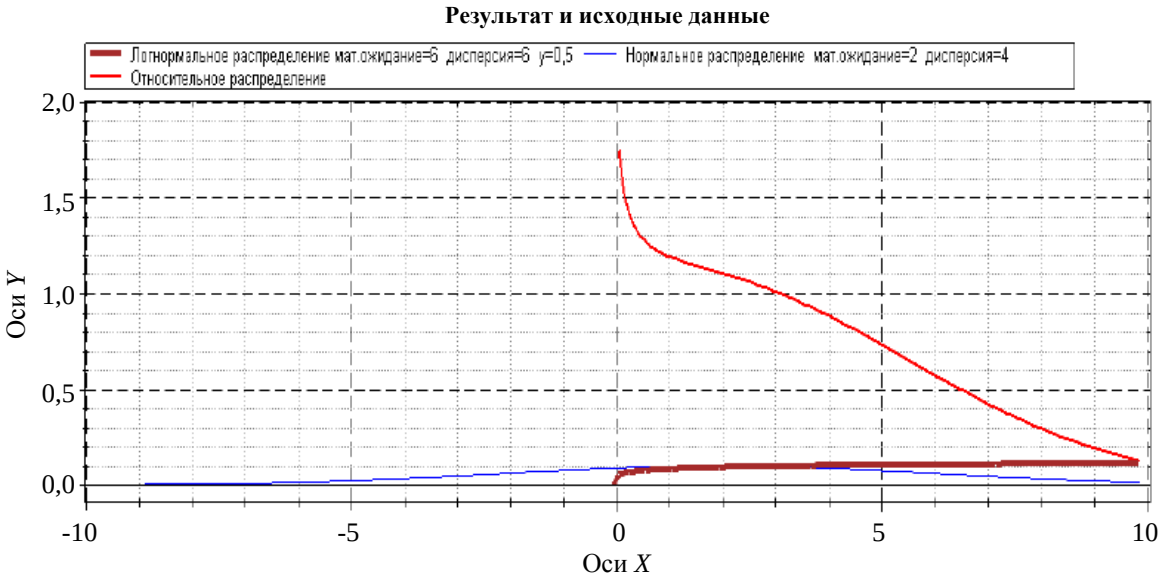


Рис. 2. Плотность распределения вероятностей мгновенных значений информационного показателя помехозащищенности (относительное распределение

Анализ полученных данных показывает, что форма (следовательно, и энтропия) ПРВ функционального отношения ПРВ помехи и сигнала существенно отличается от исходных законов распределения помехи и сигнала. При этом ПРВ вида (1) может быть и многомодальной (при одномодальных законах распределения помехи и сигнала), что влечет за собой значительный разброс в оценке возможных значений информационных потерь.

Заключение

В любом случае применение описанного методического подхода при реальных (в том числе и многомодальных) законах распределения сигналов и помех повышает достоверность оценки помехозащищенности приемника.

Применение инструментально-расчетного метода оценки относительных информационных потерь при воздействии радиопомех на цифровые радиоприемные устройства с помощью современной цифровой измерительной техники на входе и выходе цифровых радиоприемных устройств существенно повышает адекватность современных моделей оценки влияния вида и параметров помех на качество приема или радиоэлектронного подавления цифровых каналов связи.

Литература

1. *Владимиров В. И., Владимиров И. В., Наметкин В. В.* Избранные вопросы радиоэлектронного подавления цифровых сигналов систем радиосвязи. — Воронеж: ВАИУ, 2010. — 119 с.
2. *Душкин А. В.* Некоторые прикладные вопросы информационной безопасности систем обработки информации // Современные наукоемкие технологии. 2016. № 8/1. С. 41—45.
3. *Панычев С. Н.* Когнитивный алгоритм корреляционно-фильтровой обработки сложных сигналов на фоне гауссовых шумов: мат. XX Междунар. конф. "Радиолокация, навигация, связь" (RLNC 2014). — Воронеж, ВГУ, 2014. С. 1053—1065.
4. *Душкин А. В.* Применение методов прямой фильтрации в решении оптимизационных задач // Вестник Воронежского института ФСИН России. 2013. № 1. С. 68—70.
5. *Хибель М.* Основы векторного анализа цепей. — М.: МЭИ, 2009. — 500 с. [Электронный ресурс]. http://library.distudy.ru/books/gonorovskiy/pages/109.html. (дата обращения: 21.06.2022).
6. *Тупота В. И. и др.* Способ оценки качества маскирующего акустического (вибро-акустического) шума. Патент № 2350023 РФ. Опубл. в БИ 20.03.2009 г.
7. *Гуменюк А. С.* Алгоритмы анализа структуры сигналов и данных: монография. — Омск: ОмГТУ, 2010. — 272 с.

Substantiation of the instrumental-calculative method for assessing information losses in digital receivers of technical reconnaissance equipment

A. V. Dushkin, Yu. V. Savchenko
National Research University "Moscow Institute of Electronic Technology",
Zelenograd, Moscow, Russia

V. A. Shcherbakov, I. S. Rekunkov
Military Academy of strategic Missile forces named after Peter Great,
Balashikha, Moscow region, Russia

The article presents the results of the substantiation of the instrumental-calculative method for estimating information losses in the receivers of digital reconnaissance means based on the procedures for measuring the probability distribution densities of instantaneous values of useful signals and interference at the receiver input. The probabilistic criteria for information losses are substantiated and procedures for their quantitative evaluation at the input and output of the receiver using modern measuring equipment are proposed. An example of the application of the information criterion in the practice of testing a receiving device for noise immunity is given.

Keywords: noise immunity, information loss, reconnaissance equipment.

Bibliography — 7 references. *Received February 14, 2023*

УДК 004.056.5
DOI: 10.52190/2073-2600_2023_1_47
EDN: QSKKFT

Математическое моделирование защитных экранов для предотвращения утечки информации по техническим каналам в радиодиапазоне

Р. В. Мещеряков, д-р техн. наук
Институт проблем управления им. В. А. Трапезникова Российской академии наук, Москва, Россия

В. П. Лось, д-р воен. наук
МИРЭА — Российский технологический университет, Москва, Россия

В. А. Щербаков, д-р техн. наук; *И. С. Рекунков*, канд. техн. наук
Военная академия РВСН им. Петра Великого, г. Балашиха, Московская обл., Россия

Предложены несколько видов дисперсионных экранов, которые могут быть использованы в целях защиты информации, которая содержится в широкополосных информационных сигналах при одновременном обеспечении окон прозрачности в узких полосах частот, т. е. при наличии информационной системы, обладающей радиоканалом приема-передачи информации.

Ключевые слова: технические каналы утечки информации, информационные объекты, защитные экраны.

Средства несанкционированного доступа к конфиденциальной информации зачастую используют несовершенства системы обработки, передачи и хранения информации, проявляющиеся в появлении нежелательных, с точки зрения безопасности, электромагнитных излучений [1—7]. В целях нейтрализации радиотехнических электромагнитных каналов утечки информации применяют активные и пассивные методы, имеющие свои недостатки и преимущества. В ряде случаев использование активных методов защиты информации не всегда возможно или трудно реализуемо.

Пассивные методы защиты информации, базирующиеся на подавлении электромагнитных сигналов, лишены подобных недостатков. Одним из перспективных пассивных методов, основанных на подавлении информационного сигнала, является электромагнитное отражающее и поглощающее экранирование. В связи с увеличением мощностей вычислительных и телекоммуникационных систем, использованием сложных модуляций сигналов, увеличением спектральных диапазонов рабочих частот, актуальными являются разработка и исследование характеристик широкополосных защитных экранов, а также поиск и применение новых видов материалов для поглощения электромагнитной энергии. Разработка радиопоглощающих материалов требует учета явлений отражения электромагнитных волн от границы раздела, поглощения и рассеяния излучения. Это, в свою очередь, требует решения задачи обоснования соответствующей методологической базы для подобных исследований, а также новых математических и алгоритмических методов обеспечения систем анализа и обработки полученной информации, а также адаптации уже имеющихся моделей и методов решения задач системного анализа электромагнитных явлений.

Одним из способов защиты информационных объектов является создание систем экранов и экранирующих оболочек, уменьшающих уровень собственных излучений источников информации в диапазоне частот, в котором данные излучения достигают максимального амплитудного значения и несут в себе наивысшую информативность.

Мещеряков Роман Валерьевич, профессор, заведующий лабораторией.
E-mail: meshcherykov.roman@gmail.com
Лось Владимир Павлович, профессор, директор центра исследования проблем кадрового обеспечения отрасли информационной безопасности.
E-mail: tyshuk@mirea.ru
Щербаков Виталий Алексеевич, заместитель начальника кафедры.
E-mail: svasvarog@yandex.ru
Рекунков Иван Сергеевич, докторант кафедры.
E-mail: ivan.grek.1982@mail.ru

Статья поступила в редакцию 14 февраля 2023 г.

Такой способ экранирования является пассивным и скрытным для обнаружения. Система экранов не призвана демаскировать местоположение источника информации, тем не менее, существующие в настоящий момент системы приема радиосигналов отличаются высокой степенью чувствительности и обладают способностью, производить выделение и обработку внутрисистемных сигналов конфиденциальных информационных объектов даже в том случае, когда их местоположение не локализовано с требуемой точностью. При этом, точность может изменяться в интервале от единицы метров до десяти километров и зависит от местоположения каналов утечки информации (воздушных, наземных, надводных, космических).

В настоящее время усилия разработчиков направлены на создание и изучение широкополосных по свойствам и малогабаритных по размеру материалов поглощающего класса. Актуален стоит вопрос исследования экранирующих замкнутых оболочек и экранов, обладающих хорошими дисперсионными свойствами, для объектов информационных технологий, использующих устройства связи, навигации и радиолокации.

Цель работы — разработка информационных моделей для исследования параметров электромагнитных экранов, предназначенных для устранения технических каналов утечки информации, и выработка рекомендаций для их использования в роли пассивного средства защиты информации.

Постановка задачи исследований

Одной из возможностей реализации защитных экранов, обладающих хорошими дисперсионными свойствами, являются периодические металлодиэлектрические экраны, имеющие в своем составе резонансные элементы щелевого или проволочного типа, а также их различные комбинации. Такие экраны, благодаря справедливости принципа двойственности [1], обладают аналогичными характеристиками рассеяния при замене электрического и магнитного полей на своих поверхностях. Так, по принципу двойственности происходит для случая, когда первичные поля связаны соотношениями

$$E_2^0 = -H_1^0, \quad (1)$$

$$H_2^0 = E_1^0. \quad (2)$$

Полные поля E_1, H_1 и E_2, H_2 в полупространстве $z > 0$ будут взаимосвязаны:

$$E_2 = H_1 - H_1^0, \quad (3)$$

$$H_2 = -\left(E_1 - E_1^0\right). \quad (4)$$

В работах [2—13] показано, что периодические металлодиэлектрические экраны могут обладать свойствами резонаторов с непрерывным частотным спектром, а также представлять собой основу для создания "невидимых" поглощающих экранов. В данной работе описан подход к исследованию ряда свойств подобных периодических металлодиэлектрических экранов, основанный на принятии в качестве допущения их однородности. Тогда периодические металлодиэлектрические экраны, геометрия которых представлена на рис. 1, по всему своему объему будут характеризоваться отрицательными величинами констант магнитной и диэлектрической проницаемости для каждого частотного диапазона.

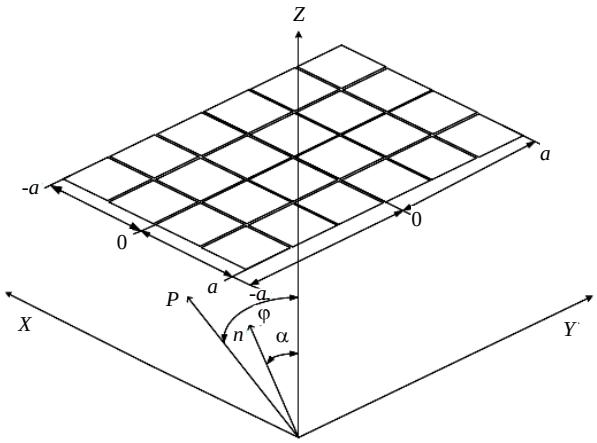


Рис. 1. Геометрия периодического металлодиэлектрического экрана

На рис. 2 представлена геометрия единичных элементов, на периодическом повторении которых происходит построение планарной и объемной конструкции металлодиэлектрического экрана.

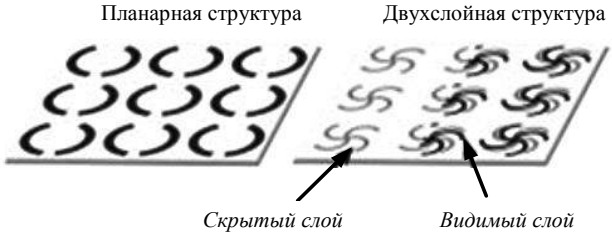


Рис. 2. Единичные элементы конструкции металлодиэлектрического экрана

На рис. 3 представлена структура перспективного защитного экрана.

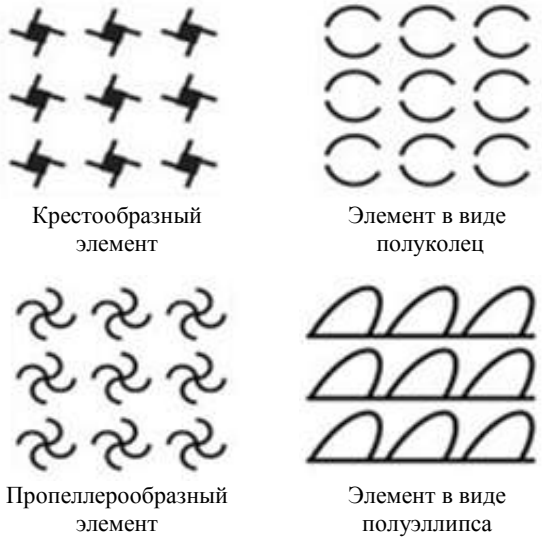


Рис. 3. Структуры защитного экрана

Для исследования излучающих свойств экранов, предназначенных для обеспечения защиты и сохранности информации в возможных электромагнитных каналах утечки, необходимо проведение моделирования и последующей оценки соответствующих каждому типу экрана его амплитудно-частотных характеристик. Для распознавания конфиденциальной информации, подвергающейся утечке со стороны нарушителя системы безопасности, решающую роль имеют фазовые характеристики.

Для определения характеристик нелинейного рассеивания электромагнитной волны на защитном экране необходимо получить амплитудно-фазовую характеристику плотности тока на поверхности экрана для определенных принятых граничных условий с учетом вида аппроксимирующей функции для ВАХ сосредоточенного нелинейного рассеивания.

Для моделирования характеристик электромагнитного излучения широкое распространение и развитие получили два класса методов математического моделирования — матричные методы моделирования и методы эквивалентных схем.

Моделирование характеристик защитных экранов

Применение матричных методов моделирования дает возможность определения вторичных волн, отраженных защитным экраном на частотах облучающей монохроматической электромагнитной волны, а также описания процесса рассеивания электромагнитных волн на частотах нелинейных эффектов апертуры экрана.

На рис. 4 представлены результаты моделирования амплитудно-частотной характеристики двухслойного защитного экрана со слоями взаимно-дополнительного типа, полученной методом эквивалентной схемы Тевенена с помощью математического пакета *MathCAD*.

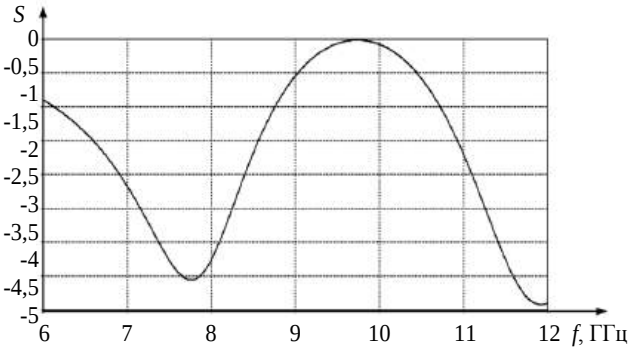


Рис. 4. Амплитудно-частотная характеристика двухслойного защитного экрана со слоями взаимно-дополнительного типа

Для исследования предлагаемой конструкции двухслойных защитных экранов со слоями взаимно-дополнительного типа также был использован метод функциональных рядов Вольтера. Преимуществом данного метода является возможность получения хорошо интерпретируемого и наглядного решения. При использовании метода функциональных рядов Вольтера отклик со стороны защитного экрана, обладающего нелинейными свойствами, и для которого справедливы условия причинности на определенное воздействие $\varepsilon(t)$, представляющего собой ЭДС, наведенную в антенне радиопередающего устройства, может быть определен выражением

$$\nu(t)=\sum_{n=0}^{\infty}\nu_n(t)=\sum_{n=0}^{\infty}\int_{E_n}h(t;\tau_{1,n})\prod_{i=1}^{n}\xi(\tau_i)\,d\tau_i\,, \qquad (5)$$

где $\nu_n(t)$ — однородный регулярный функционал *n* степени;

E_n — *n*-мерное евклидово пространство;

$h(t;\tau_{1,n})$ — ядро функционального ряда Вольтера *n*-го порядка, которое может быть интерпретировано в качестве импульсной характеристики моделируемой системы, описывающей систему, обладающую *n*-й степенью нелинейности.

В рабочем диапазоне частот данной характеристике будет соответствовать некоторая нелинейная передаточная функция $H(i\omega_1, i\omega_2, \ldots, i\omega_n)$, которая связана с ядром n-мерного ряда $h(t; \tau_{1,n})$ при помощи прямого преобразования Фурье.

На рис. 5 представлены результаты моделирования коэффициентов рассеяния двухслойного защитного экрана толщиной 1 мм со значением нижней собственной частоты одиночного элемента 10 ГГц, полученные методом Вольтера при помощи программного обеспечения CST.

На рис. 6 представлены результаты моделирования коэффициентов рассеяния двухслойного защитного экрана толщиной 1 мм со значением нижней собственной частоты одиночного элемента 10 ГГц, полученные подстановочным методом при помощи программного обеспечения CST.

На рис. 7 представлены результаты моделирования коэффициентов рассеяния двухслойного защитного экрана толщиной 1 мм со значением нижней собственной частоты одиночного элемента 10 ГГц при межслойном расстоянии, составляющем 10 мм, полученные модифицированным методом функциональных рядов Вольтера при помощи программного обеспечения CST.

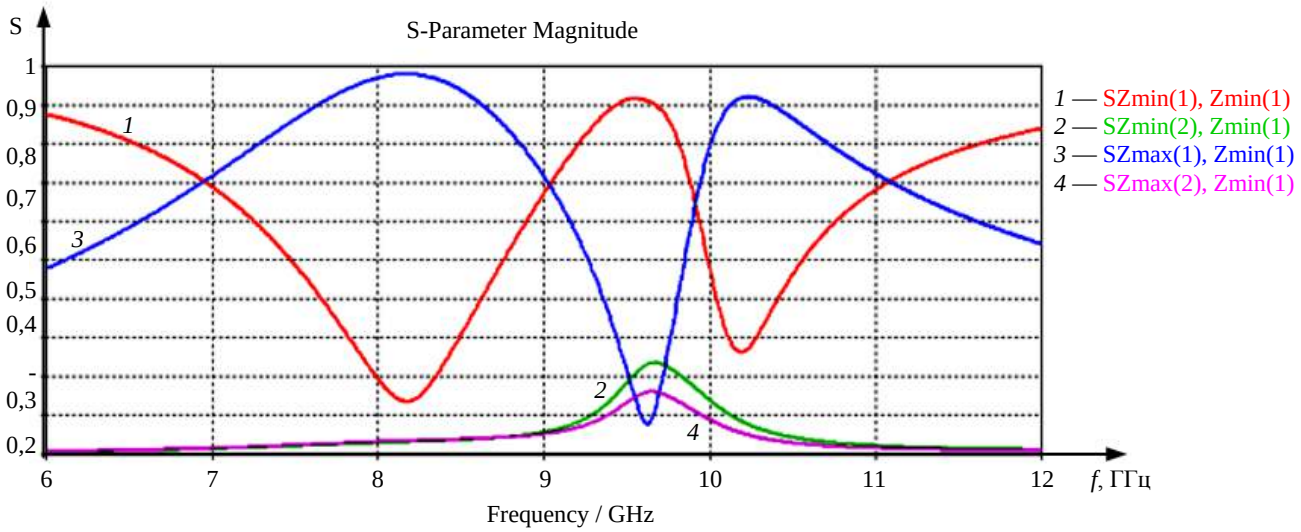


Рис. 5. Коэффициенты рассеяния двухслойного защитного экрана

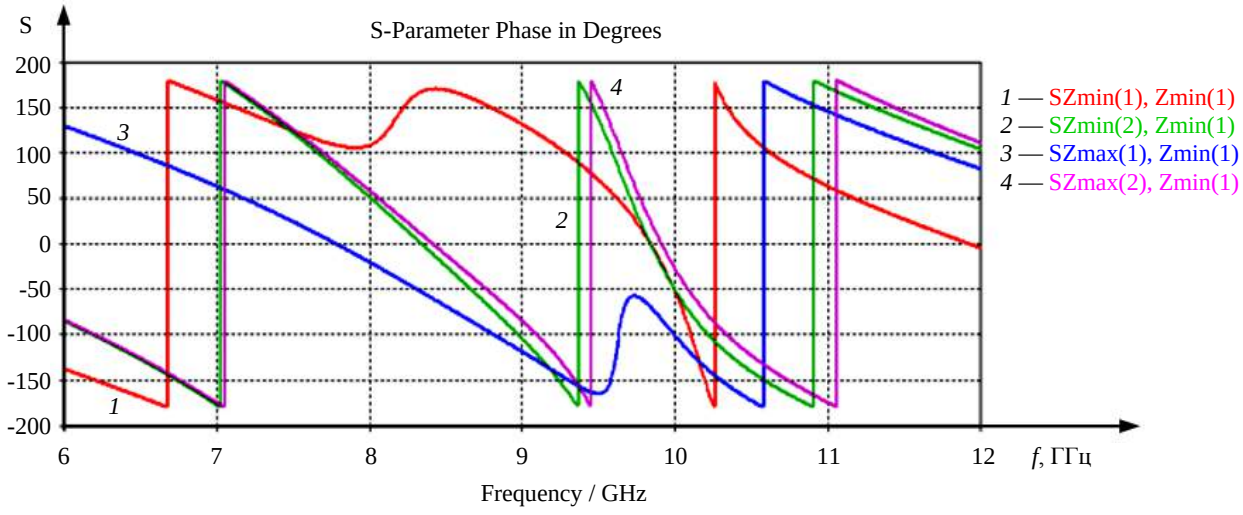


Рис. 6. Коэффициенты рассеяния двухслойного защитного экрана

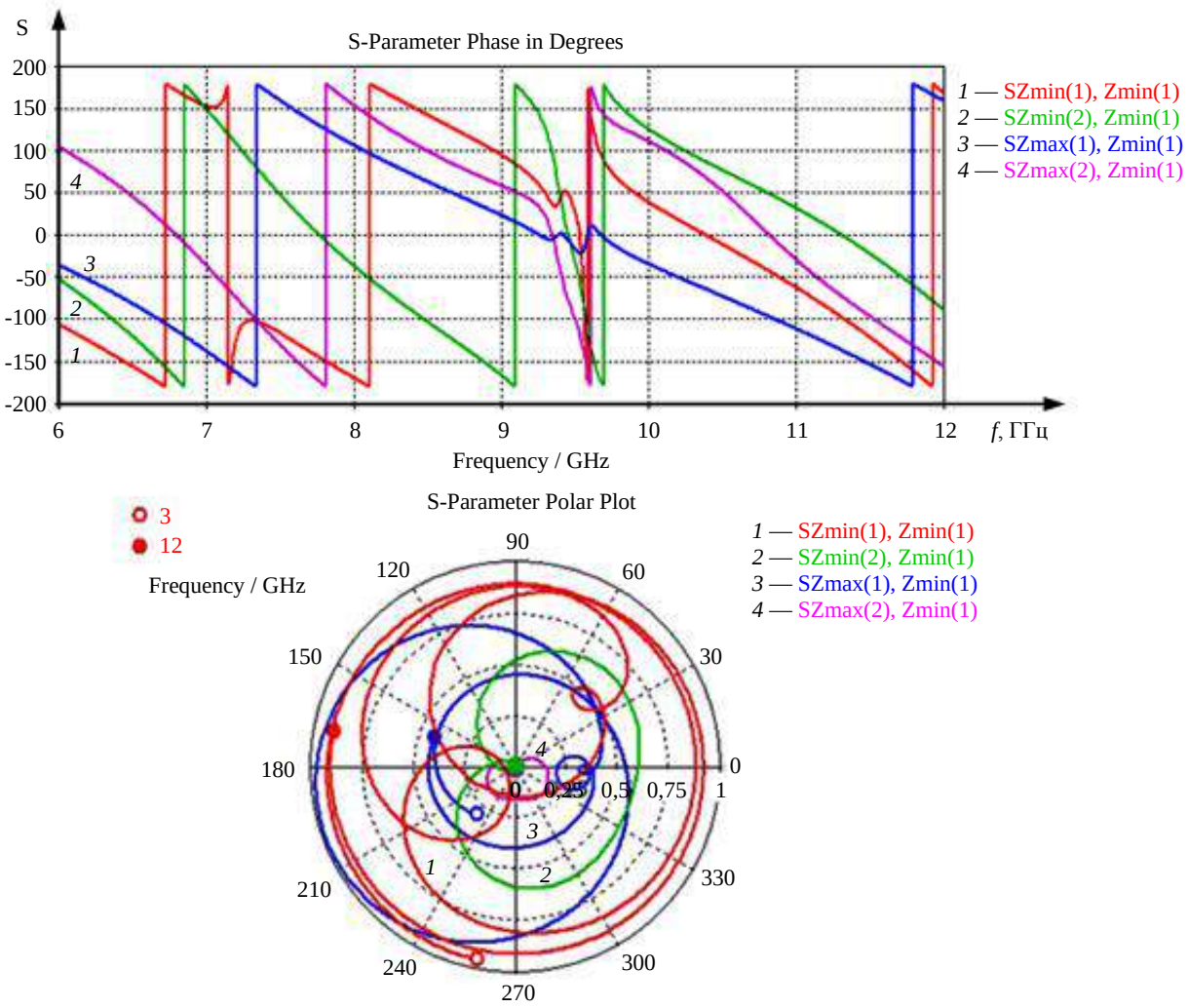


Рис. 7. Коэффициенты рассеяния двухслойного защитного экрана при межслойном расстоянии 10 мм

Заключение

В данной работе были проведено информационное моделирование характеристик и предложены конструкции планарных защитных экранов и двухслойных защитных экранов взаимнодополнительного типа для устранения технических каналов утечки информации. Проведенные исследования показали, что защитный экран в своей физической интерпретации представляет пространственно-частотный фильтр, при прохождении которого информационный сигнал претерпевает амплитудные и фазовые искажения, а также частично отражается. Изменения информационного сигнала при этом подобны по своему принципу искажениям в системах кодирования радиотехнического сигнала. При осуществлении восстановления импульсных характеристик информационного сигнала, частично отраженного, но и частично-пройденного через такой экран, выделение из него информации затруднено в связи с неизвестными параметрами пространственно-частотного фильтра. Предлагаемые виды экранов могут быть использованы для защиты конфиденциальной информации в информационной системе, обладающей радиоканалом приема—передачи информации.

Литература

1. *Петров Б. М.* Электродинамика и распространение радиоволн: учебник для вузов. — М.: Горячая линия-Телеком, 2007. — 558 с.
2. *Wang J. F., Qu S. B., Fu Z. T. et al.* Three-dimensional metamaterial microwave absorbers composed of coplanar magnetic and electric resonators // Progress in electromagnetics research letters. 2009. V. 7. P. 15—24.
3. *Меньшаков Ю. К.* Теоретические основы технических разведок: учеб. пособие. — М.: МГТУ им. Н. Э. Баумана, 2008. — 536 с.
4. *Душкин А. В.* Программно-аппаратные средства обеспечения информационной безопасности. — М.: Горячая линия — Телеком, 2016. — 248 с.
5. *Душкин А. В.* Методологические основы построения защищенных автоматизированных систем. — Воронеж: Научная книга, 2016. — 76 с.

6. *Авсентьев О. С.* Модель оптимизации процесса передачи информации по каналам связи в условиях угроз ее безопасности // Телекоммуникации. 2016. № 1. С. 28—32.

7. *Хорев А. А.* Техническая защита информации: учебное пособие для студентов вузов: в 3 т. — Т. 1: Технические каналы утечки информации. — М.: НПЦ "Аналитика", 2008. — 436 с.

8. *Догматырко Д. Г., Козачок Н. И., Литвиненко В. П.* Основные методы математического и экспериментального моделирования эффекта нелинейного рассеивания электромагнитных волн // Вестник Воронежского государственного технического университета. 2010. № 1. С. 30—37.

9. *Harger R. O.* Harmonic radar systems for near-ground in-foliage nonlinear scatterers // IEEE Trans. 1976. V: AES-12. № 2. P. 230—245.

10. *Opitz C. L.* // Microwaves. 1976. № 5. P. 38—45.

11. *Flemming M. A., Mullins F. H., Watson A. W. D.* Harmonic radar detection systems // Proceedings of the IEE International Conference RADAR-77. 1977. P. 552—554.

12. *Harrison C. W., Aronson E. A.* On the evaluation of potential intergrals occurring in antenna theory using digital computers // IEEE Trans. 1967. V. 15. № 4. P. 576. DOI: 10.1109/TAP.1967.1138960.

13. *Семенихина Д. В.* Нелинейный эффект в высокочастотных трактах антенн. В кн. Теория и техника антенн МКТТ'95. — Харьков. 1995. — 345 с.

14. *Watt J.* Equivalent circuits might look distinctly odd, but they do simplify circuit design // Electronics & Wireless world. 1987. V. 93. № 1622. P. 1201—1205.

Mathematical modeling of protective screens to prevent information leakage through technical channels in the radio range

R. V. Meshcheryakov
Institute of Management Problems named after V. A. Trapeznikov of the RAS, Moscow, Russia

V. P. Los
MIREA — Russian Technological University, Moscow, Russia

V. A. Shcherbakov, I. S. Rekunkov
Military Academy of strategic Missile forces named after Peter Great, Balashikha, Moscow region, Russia

The article proposes several types of dispersion screens that can be used to protect information contained in broadband information signals while providing transparency windows in narrow frequency bands, that is, in the presence of an information system with a radio channel for receiving and transmitting information.

Keywords: technical channels of information leakage, information objects, protective screens.

Bibliography — 14 references. *Received February 14, 2023*