ISSN 2413-3582

Информационно-методический журнал

INSIDE
ЗАЩИТА ИНФОРМАЦИИ

WWW.INSIDE-ZI.RU

№ 2 (116)
2024
март – апрель

ЦИФРОВАЯ ЭПОХА КАК ИМПЕРАТИВ СМЕНЫ СТАРОЙ ПАРАДИГМЫ ИБ РОССИИ

СПЕЦИАЛИЗИРОВАННЫЙ ХОЛДИНГ
ЛАБОРАТОРИЯ ППШ

РеволЭМС

ПЕРЕГОВОРНАЯ КАБИНА
В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

ПКЗ–2У «СЕЛЕКТОР»

ПРЕДНАЗНАЧЕНА ДЛЯ ПРОВЕДЕНИЯ ЗАКРЫТЫХ СОВЕЩАНИЙ ИЛИ ПЕРЕГОВОРОВ

(в том числе с использованием телефонных аппаратов специальной связи, в которых озвучиваются сведения, содержащие государственную тайну)

ПОЛНЫЙ КОМПЛЕКС РАБОТ:
от монтажа до выдачи Аттестата соответствия требованиям безопасности информации

РЕКОМЕНДУЕТСЯ ДЛЯ РАЗМЕЩЕНИЯ:

- в государственных учреждениях и коммерческих организациях, работающих с государственной тайной;
- для ведения переговоров директорам и сотрудникам секретных производств и конструкторских бюро оборонно-промышленного комплекса;
- сотрудникам прокуратуры и силовым ведомствам

ПРОИЗВЕДЕНО В РОССИИ

121596, г. Москва, ул. Горбунова, д.2, стр.2 ◇ +7(499)700-8878 ◇ www.revolemc.ru

Информационно-методический журнал
INSIDE
ЗАЩИТА ИНФОРМАЦИИ

Информационно-методический журнал «ЗАЩИТА ИНФОРМАЦИИ. ИНСАЙД»

№ 2 (116) март – апрель 2024 г.
от 02.04.2024

Выходит 6 раз в год.
Очередной № 3'2024 выйдет 05.06.2024

Зарегистрирован Министерством РФ по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-18089 от 26 мая 2004 г.

ISSN 2413-3582

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ
ООО «Издательский Дом «Афина»

194017, Санкт-Петербург,
пр. Тореза, д. 98, корп. 1, оф. 315
Тел.: +7 (921) 958-25-50,
+7 (911) 921-68-24,
e-mail: magazine@inside-zi.ru
http://www.inside-zi.ru

Журнал включен:
в перечень ВАК при Минобрнауки России;
в базы данных РИНЦ (http://elibrary.ru);
в базы данных
и в Реферативный журнал ВИНИТИ РАН

Подписной индекс журнала в каталоге:
«Почта России» ПИ463
https://podpiska.pochta.ru/

РЕДАКЦИЯ
194017, Санкт-Петербург,
пр. Тореза, д. 98, корп. 1, оф. 315

Главный редактор:
С. А. Петренко, *д. т. н., профессор*
Ответственный редактор: **А. В. Архипов**
Подписка, распространение: **С. В. Иванова**
Реклама, выставки: **А. Ф. Солодилова**
Арт-директор: **Н. В. Резников**

Отпечатано в типографии «ОнлайнКопи»
Москва, Байкальская улица, д. 7, стр. 7
Тираж: 1500 экз.

Цена свободная

СОДЕРЖАНИЕ

СОБЫТИЯ

С 1 марта заработал запрет рекламы VPN

1 марта 2024 года в России вступил в силу запрет на популяризацию средств обхода интернет-блокировок (Приказ Роскомнадзора от 8 ноября 2023 года № 168). Теперь доступ к материалам, популяризирующим подобные средства или рекламирующим средства обхода блокировок, будет блокироваться Роскомнадзором.

Исключение составили статистическая, научная и научно-техническая информация о способах и методах обеспечения доступа к ограниченным ресурсам и сетям.

Приказ РКН действителен до 1 сентября 2029 года.

Сбер предложил создать ассоциацию банков стран БРИКС в сфере кибербезопасности

Сбер выступил с предложением создать ассоциацию банков стран БРИКС в сфере кибербезопасности, сообщил первый заместитель председателя правления Сбербанка Александр Ведяхин на семинаре по финансированию устойчивого развития.

Странами БРИКС уже не раз поднимался вопрос кооперации в сфере кибербезопасности, в частности, не так давно представители центральных банков объединения обсудили возможный обмен информацией о компьютерных атаках и киберугрозах, с которыми столкнулись страны-члены.

Инициатива создания отдельной ассоциации однозначно заслуживает внимания, прокомментировал инициативу член комитета Госдумы по информационной политике, информационным технологиям и связи Антон Немкин: «Подобные международные организации уже функционируют в ряде стран и давно показали свою эффективность. Важно, что инициатива исходит от банковского сектора. Не только в России, но и в ряде других стран банки становятся главными драйверами развития ИТ-технологий, аккумулируя в себе терабайты критически важной информации: от персональных данных пользователей до конфиденциальных данных госсектора».

ОЦЕНКИ И ПРОГНОЗЫ

Киберпреступность в России и СНГ: анализ, тренды, прогнозы

Исследователи компании F.A.C.C.T. представили новый аналитический отчет «Киберпреступность в России и СНГ. Анализ, тренды, прогнозы. 2023–2024 гг.».

Это исследование является наиболее полным источником стратегических и тактических данных о киберугрозах, актуальных для России и СНГ в период острого геополитического конфликта, о тактиках, инструментах и активности атакующих.

Специалисты платформы кибер разведки F.A.C.C.T. Threat Intelligence выделили 14 прогосударственных хакерских групп, активно работавших в 2023 году на территории России и стран СНГ. Чаще всего прогосударственные хакерские группы (APT) атаковали Россию (28 атак), Азербайджан (6 атак) и Беларусь, Киргизию, Казахстан (по 4 атаки). Целями являлись госучреждения, организации, связанные с критически важной инфраструктурой, военные учреждения и предприятия оборонно-промышленного комплекса.

Открытием года стали группы двойного назначения, которые преследуют как финансовые, так и политические цели. Наиболее яркий пример – преступный синдикат Comet (Shadow) – Twelve, в котором Comet (Shadow) выступает в роли вымогателя (требует выкуп за расшифровку и нераспространение похищенных данных), а Twelve – в роли хактивиста-диверсанта, уничтожающего ИТ-инфраструктуру жертвы без выставления финансовых требований.

В 2023 году наиболее популярными вредоносными программами в письмах стали шпионская программа Agent Tesla и стилеры FormBookFormgrabber и Loki PWS.

Одной из наиболее активных групп, атакующей компании в России и СНГ, в прошлом году были операторы трояна DarkWatchman.

Эксперты F.A.C.C.T. обнаружили в 2023 году около 300 облаков логов (*Underground Cloud of Logs*, UCL), через которые проходят огромные потоки украденных данных, полученных в основном с помощью вредоносных программ-стилеров.

Что думают россияне о своей ИТ-безопасности

Сохранность личной информации – актуальная проблема современного цифрового мира. ВЦИОМ выяснил, что семь из десяти интернет-пользователей (68 %) опасаются за сохранность своих персональных данных, таких как данные банковского счета, пароли от почты или социальных сетей. В том числе каждый пятый отметил, что «очень опасается» кражи личных данных (23 %), а почти половина – что «скорее опасаются» (45 %). Подобные тревоги в большей степени присущи женщинам (74 % vs 61 % мужчин), молодежи до 24 лет (70 %) и россиянам 45–59 лет (74 %).

Около трети пользователей интернета (31 %) отметили, что в целом не испытывают переживаний из-за возможного взлома их аккаунтов или утечки ПДн.

Большая часть работающих россиян (83 %) убеждены: их ПДн и данные компании, где они работают, под надежной защитой. Каждый десятый считает, что должный уровень безопасности личных данных на рабочем месте не обеспечивается.

Вопрос защиты личных устройств от онлайн-угроз, таких как вредоносное ПО или кибератаки, – тема для россиян скорее сложная. Только 14 % респондентов абсолютно уверены в своей способности защитить компьютер или смартфон от таких угроз. Еще 34 % «скорее уверены» в этом. Достаточно большая часть наших сограждан (44 %) признались, что они не смогут обезопасить свои гаджеты от вредоносных программ или кибератак. Чем старше россияне, тем чаще они так думают: если среди молодежи 18–24 года показатель составляет 26 %, то в группе старше 60 лет – 52 %.

В российском обществе нет единого мнения о влиянии новых технологий на безопас-

ность персональных данных. Каждый третий (33 %) полагает, что новые технологии скорее не повлияют на сохранность личной информации и персональных данных. Еще треть россиян (32 %) уверены, что новые технологии скорее понизят сохранность личной информации и персональных данных. Пятая часть россиян (23 %) настроены оптимистично, в новых технологиях они видят способ повысить сохранность личной информации.

ИСТОРИЯ

Жизнь, посвященная шифрам

Дэвид Кан, журналист и историк, раскрывший тайный мир криптологии в своем бестселлере 1967 года «Взломщики кодов» и других книгах, скончался 23 января 2024 года в своем доме в Бронксе. Ему было 93 года.

Ученый родился в Манхэттене 7 февраля 1930 года. Его отец, адвокат, и мать, владелица стекольного завода, воспитывали троих детей на Лонг-Айленде.

В возрасте 13 лет Кан, проходя мимо местной библиотеки в Грейт Нек, Нью-Йорк, заметил книгу «Тайное и срочное: История кодов и шифров» военного историка Флетчера Пратта. Это произведение «остановило его на месте», рассказал он газете The Washington Post много лет спустя.

Увлекшись этой книгой, он стал любителем криптологии и сохранил этот интерес на протяжении всей своей карьеры журналиста. Во время развития своего интереса к криптологии Кан создавал словесные головоломки, которые публиковались в комиксах 1940-х годов. В подростковом возрасте он вступил в переписку с Уильямом Ф. Фридманом, именуемым отцом современной американской криптологии, который поддерживал его интерес к этой области.

В 1951 году Кан получил степень бакалавра социальных наук в Университете Бакнелл в Льюисберге, Пенсильвания, где работал в студенческой газете. Из-за плохого зрения он был непригоден к военной службе во время войны в Корее и начал свою карьеру журналиста.

В 1960 году два математика, работавшие в АНБ, Уильям Х. Мартин и Бернон Ф. Митчелл, перешли на сторону СССР и раскрыли ряд фактов о деятельности агентства по сбору информации. В частности, они утверждали, что США взломали шифры 40 других стран, включая многочисленных союзников.

В условиях шумихи, Кан предложил журналу New York Times статью об истории криптологии, ставшую отправной точкой для его первой и самой известной книги.

«Взломщики кодов», представленная как «первая всеобъемлющая история секретной коммуникации от древних времен до порога космической эры», сразу же стала сенсацией.

На более чем 1000 страницах авторитетного и легко читаемого текста, без всяких разрешений на доступ к секретной информации, Кан провел читателя через тысячелетия истории: от времен клинописи до эпохи Наполеона, через расшифровку телеграммы Циммермана во время Первой мировой войны и дешифровку кодов Второй мировой войны до современной деятельности АНБ.

«Никто не писал об этом раньше», – справедливо отметил Николас Рейнольдс, автор книги «Нужно знать: Вторая мировая война и возникновение американской разведки». – «Он открыл дверь в совершенно новое поле, в основном, в историю радиоразведки».

При этом Кан столкнулся с нежеланием многих чиновников правительства США оставить эту дверь открытой. Журналист Джеймс Бэмфорд описал в своей книге 1982 года «Дворец головоломок: отчет о самом секретном агентстве Америки» шаги, которые АНБ рассматривала для блокирования опубликования работы Кана или ограничения объема раскрываемой им информации. Отклоненные в конечном итоге меры включали в себя:

- назначение Кана на должность в правительстве, что позволило бы применять определенные уголовные статьи в случае публикации его произведения;
- подачу «тайных служебных заявок» против автора (может означать все что угодно, начиная от физического наблюдения и заканчивая операциями под прикрытием);
- осуществление «тайного проникновения» в дом Кана на Лонг-Айленде.

Согласно Бэмфорду, издатель Кана, Macmillan, предоставил весь манускрипт в Министерство обороны, которое ответило, что «публикация книги не будет соответствовать национальным интересам». В итоге Macmillan и Кан согласились удалить несколько абзацев, касающихся сотрудничества АНБ с британской разведкой. Ситуация изменилась со временем: по мере того как Кан продолжал публиковать пользовавшиеся уважением книги о радиоразведке, а миссия АНБ в сфере национальной безопасности становилась понятнее общественности, обе стороны нашли путь к взаимному уважению.

В 1990-х годах Уильям Кроуэлл, тогдашний заместитель директора АНБ настаивал на том, чтобы утвердить Кана научным сотрудником агентства. «Во всей стране я не мог найти никого в сфере гражданского сектора, кто сравнился бы с ним по знаниям в области криптографии и криптоанализа», – подчеркнул Кроуэлл.

В 1974 году Кан получил докторскую степень по современной истории в Оксфордском университете в Англии, где его диссертация стала основой для книги «Шпионы Гитлера: Немецкая военная разведка во Второй мировой войне» (1978). В ходе подготовки книги Кан взял интервью у дюжины высокопоставленных нацистов. «Я был уверен, что с их хваленой эффективностью они должны были купаться в успехе, но на деле их ждала череда неудач», – делился он с The Post своим мнением о разведке Гитлера. «Их информация была неполной и неточной, отчасти из-за того, что Гитлер ставил на руководящие посты в разведке некомпетентных людей. Но даже будь у него в руках идеальные разведданные, его высокомерие не позволило бы ему поверить в то, что советские войска не такие уж некомпетентные и слабые и не развалятся при первом же ударе».

Среди последующих книг, написанных Каном, были «Захват Энигмы: Гонка за взломом кодов немецких подводных лодок, 1939–1943» (1991) и «Читатель джентльменской почты: Герберт О. Ярдли и рождение американской криптографии» (2004).

Двадцать лет назад Кан начал искать постоянный дом для своих бумаг и обширной коллекции книг и артефактов из области разведки, среди которых, например, имелось письмо Наполеона Бонапарта от 1806 года с просьбой к своему сыну вести переписку с использованием шифра. Для хранения этого наследия он выбрал Национальный криптологический музей АНБ.

При подготовке новостей использованы материалы сайтов facct.ru, novostiitkanala.ru, sber.ru, wciom.ru.

Цифровая эпоха

как императив смены старой парадигмы информационной безопасности России

En

The Digital Age as an Imperative to Change the Current Paradigm of Russian Information Security

V. M. Buryakov
v.m.buryakov@mtuci.ru
Moscow Technical University of Communications and Informatics

Russia, having proclaimed in 2016 a course to build a digital economy and strengthen digital sovereignty, still exists in the old American paradigm of information security (C.I.A. triad) of the 1970s and a vague terminology ecosystem. The purpose of the work is a structured analysis of the above problems, the justification of the need to change the existing concept of information security in Russia and the development of a concept of digital security adequate to the new threats of the digital paradigm of the West.

The study provides a new vision of the digital space as a superposition of the anthropocentric information space and cyberspace and is a theoretical justification for the concept of a new paradigm of digital security in Russia, with the separation of cyber security and anthropocentric information security into separate independent areas.

Keywords: digital space, cyberspace, information space, digital terminology ecosystem, cyber security, cyber-physical systems, digital sovereignty, cyber sovereignty, digital security, cyber threats, information threats, network-centric architecture

УДК 004.056

Россия, провозгласив в 2016 году курс на построение цифровой экономики и укрепление цифрового суверенитета, до сих пор существует в старой американской парадигме информационной безопасности (CIA-триада) 70-х годов прошлого века и размытой терминологической экосистеме. Целью работы является структурированный анализ вышеперечисленных проблем, обоснование необходимости изменения существующей концепции информационной безопасности России и разработка концепции цифровой безопасности, адекватной новым угрозам цифровой парадигмы Запада.

Исследование дает новое видение цифрового пространства как суперпозиции антропоцентрического информационного пространства и киберпространства, а также является теоретическим обоснованием концепции новой парадигмы цифровой безопасности России с выделением кибербезопасности и антропоцентрической информационной безопасности в отдельные самостоятельные направления. Даны предложения по гармонизации цифровой терминологической экосистемы и устранению существующей путаницы в понятиях новых цифровых терминов и терминов, унаследованных из информационной эпохи.

Ключевые слова: цифровое пространство, киберпространство, информационное пространство, цифровая терминологическая экосистема, кибербезопасность, киберфизические системы, цифровой суверенитет, киберсуверенитет, цифровая безопасность, киберугрозы, информационные угрозы, сетецентрическая архитектура, кибериммунитет

Виктор Михайлович Буряков
v.m.buryakov@mtuci.ru
Московский технический университет связи и информатики

Введение

Технологическим средством цифровой парадигмы является достижение сетецентрической максимы, сформулированной в конце 90-х прошлого века визионерской американской компанией Sun Microsystems: «Everyone and everything on the planet connected to the Network» (Всё и вся на планете подключены к сети) с постепенным переходом под полный контроль искусственного интеллекта для радикального повышения нормы прибыли экономических процессов и управления человеческим поведением. Реализация стратегии Digital была начата Западом в период PAX AMERICANA, и ее успешность предполагает следование ей на условиях США (Rules-Based World Order – мировой порядок, основанный на правилах) всех государств планеты с постепенной ликвидацией их суверенитетов (политических, культурных и экономико-технологиче-

ских) как несовместимых с Digital-парадигмой сущностей, основными из которых Запад считает Россию и Китай. Цифровая парадигма Запада по своей основной сущности является машинно-сетецентрической.

По определению А. Ефремова [17], сетецентрическая система – это *«система, образованная объединенными глобальной сетью автономными автоматизированными объектами, способными действовать самостоятельно по своим алгоритмам и в тоже время самостоятельно объединяться вместе для решения общих задач»*. Сетецентрическая концепция Запада, как известно, имеет военные корни и является одной из основных угроз безопасности России.

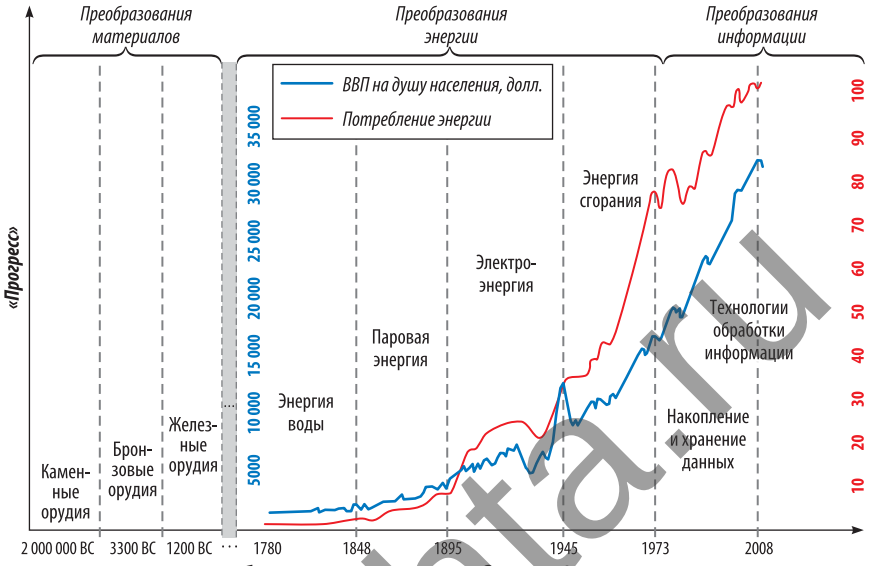


Рис. 1. ***Информационная парадигма в исторической перспективе волн Шумпетера***

Основные концепции и термины, унаследованные из информационной парадигмы

Информационная парадигма в исторической перспективе всех предыдущих волн Шумпетера из статьи [1] показана на рис. 1 с пояснениями, что парадигма состояла в освоении технологий преобразования информации (transforming information).

Первой концепцией информационной парадигмы стала концепция дихотомии информации, которая подразумевала под одним и тем же термином двоякое значение: антропоцентрическое (человекоцентрическое) и функциональное (кибернетическое). Второй концепцией (и термином) стали *«информационные технологии», также основанной на дихотомии понятия «информации»*.

Термин был впервые представлен в 1958 году, в визионерской на тот момент статье [2], в которой говорилось: *«У этой новой технологии еще нет единого общепринятого названия. Мы будем называть ее информационной технологией (ИТ)»*.

Первым этапом развития ИТ стали автоматизация информационного обмена, накопление и хранение антропоцентрической информации (communicating & storing information). Вторым этапом стали технологии обработки информации (knowledge & algorythms). Этап начался в конце 1980-х годов с появлением систем управления реляционными базами данных (*Relational Database Management System*, RDBMS), систем учета и планирования (*Enterprise Resource Planning*, ERP), систем сбыта (*Customer Relationship Management*, CRM) и аналитических систем (*Business Intelligence*, BI).

Достоин отдельного упоминания проект ЦРУ по созданию высокопроизводительной системы управления базами данных под кодовым наименованием *Oracle*. Проект осуществлял небезызвестный Ларри Эллисон, основавший потом компанию под таким же названием.

Третьей концепцией и термином стала *«информационная безопасность»*, впервые введенная в 1970-х годах Национальным институтом стандартов и технологий Департамента торговли США [3] как развитие предыдущей концепции *computer security* предынформационной эпохи. В русле принятой дихотомии информации эта концепция объединила в едином поле информационной безопасности проблемы безопасности антропоцентрической (темно-серая подсветка на рис. 2) информации и функциональной, то есть кибернетической информации (светло-серая подсветка).

Четвертой стала концепция «инфокоммуникационных технологий», введенная в 2001 году Организацией Объединенных Наций в рамках стратегии стран G7 под названием Global Digital Divide Initiative, более известная как «Устранение цифрового неравенства». Цель стратегии состояла в ускоренном подключении к Интернету населения стран Глобального Юга (бывших колоний Запада). Как стало ясно сейчас, это стремление было ни чем иным как скрытой формой «цифровой» неоколонизации.

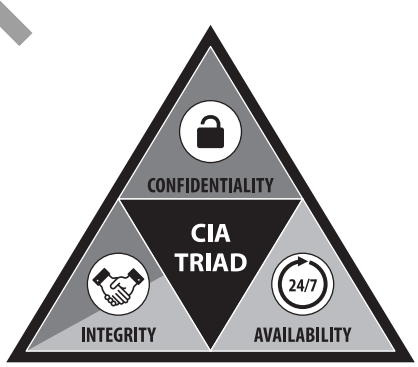


Рис. 2. ***CIA-триада***

Все западные концепции и термины информационной парадигмы в настоящее время закреплены у нас их дословными переводами в Федеральном законе от 7 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – 149-ФЗ), и лишь вместо дословного перевода западного термина *Information Security* (информационная безопасность) было использовано словосочетание «защита информации».

Национальный институт стандартов США в качестве основного содержания термина Information Security использовал триаду *«Confidentiality – Integrity – Availability»*

(Конфиденциальность – Целостность – Бесперебойность», в сокращении CIA» (см. рис. 2), и возможно эта двусмысленная аббревиатура стала причиной того, что авторы текста 149-ФЗ отклонились от дословного перевода завершающего понятия триады, зная или подозревая, какое агентство США было истинным автором термина и его концепции.

Концепции и термины с корнем «кибер» в период информационной эпохи 1973–2011 годов

Несмотря на то, что теория кибернетики Норберта Винера имела ключевое значение для информационной революции, до начала XXI века термины и названия с корнем «кибер» (cyber) в экосистеме информационной эпохи на Западе практически отсутствовали. Кибернетика фрагментировалась там в нишевые области академических наук, исследующей неосуществимые в тот период теории создания искусственного интеллекта или вопросы биологии, а также как в авангардистские идеи культуры андеграунда (в недрах которой в 1960-х годах, а именно, в книге Вильяма Гибсона «Нейроман», и появилось впервые слово «киберпространство»).

Напротив, в СССР после 1953 года и до конца следующего десятилетия кибернетика была очень популярна. С начала 1960-х годов КПСС рассматривала возможность создания взаимосвязанной компьютеризированной системы распределения ресурсов на основе принципов кибернетики. Однако вскоре на страницах газеты Washigton Post появилась статья «Перфокарта управляет Кремлем», в результате чего кибернетика попала в опалу у нового советского руководства, и к началу 70-х годов направление было закрыто.

Кибернетика как технологии самоуправления автоматизированных вычислительных систем (по Н. Винеру дословно – «управление и связь машине») в период информационной эпохи 1973–2011 годов растворилась в том, что на Западе, а потом и в России, назвали «информационными технологиями». Можно сделать предположение, что в прошлом веке слово «кибернетика» в США, как и в СССР, имело много идеологических противников в руководящих элитах, поскольку Винер распространял кибернетику не только на машины, но и на человека, социально-экономическое устройство и даже на расовые отношения. В СССР это конфликтовало с руководящей ролью КПСС, в США – с глубокими на тот момент религиозными традициями и расовыми проблемами.

Впервые термины с корнем «кибер» были кодифицированы в США после национального психологического шока 11 сентября 2001 года. В 2003 году появилась The National Strategy to Secure Cyberspace (Национальная стратегия защиты киберпространства) [2], в которой был использован термин *cyberspace* и производный от него термин *cyberspace security*.

Киберпространство определялось как «*an interdependent network, composed of hundreds of thousands of interconnected personal computers, servers, routers, switches, and fiber optic cables*» *(взаимозависимая сеть информационных технологий, состоящая из сотен тысяч связанных между собой персональных компьютеров, серверов, маршрутизаторов, коммутаторов и оптоволоконных кабелей)* [2].

Из этого определения следует, что из общей сферы информационной безопасности был выделен и назван по-другому наиболее уязвимый сегмент, не являющийся информацией в ее антропоцентрическом значении, но вызывающий при своем повреждении полную утрату этой информации и/или прекращение функционирования самоуправляемых автоматических систем объектов экономики и инфраструктур жизнеобеспечения населения.

Концепции и термины с корнем «кибер» в новую цифровую эпоху

В России аналогичный американской Национальной стратегии защиты киберпространства Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – 187-ФЗ) появился значительно позже как ответ на угрозы со стороны США в связи с их обвинениями нашей страны во вмешательстве в президентские выборы 2016 года. По информации Washington Post [5], президент Обама распорядился начать секретную операцию по внедрению в российскую инфраструктуру американского кибероружия, которое дистанционно или локально можно было бы привести в действие в случае эскалации напряженности с Москвой.

В этот период наше идеологическое расхождение с Западом стало существенно нарастать, поэтому дословных переводов западного термина *cyber* в 87-ФЗ нет. Вместо термина *cyberspace* был использован термин «критическая информационная инфраструктура». Вместо термина *cyber attack* использован термин «компьютерная атака». Аналогом американской системы National Cyberspace Security Response System стала ГосСОПКА.

В России составные термины с корнем «кибер» на официальных уровнях до настоящего времени продолжали отвергаться. В частности, проект концепции конвенции ООН, разработанный в 2011 году был назван «Об обеспечении международной информационной безопасности». В нем и во всех последующих итерациях вплоть до последней [7] термины с корнем «кибер» намеренно не использованы. Отчасти это можно объяснить и тем, что Россия по-прежнему не хочет зеркалировать кибертерминологию «The National Strategy to Secure Cyberspace», чтобы не давать лишних поводов для обвинений в скрытой подготовке сил и средств для кибератак на США.

С началом перехода Запада в цифровую экономику частота употребления там терминов с корнем «кибер» существенно возросла, поскольку основой такой экономики стали автоматические киберфизические системы или CPS (*Cyber-Physical Systems*), в которых по определению нет антропоцентрической информации или она сведена к минимуму.

В ноябре 2013 года была сделана неудачная попытка узаконить тер-

мин «кибербезопасность» через Совет Федерации РФ, где проводились парламентские слушания по обсуждению подготовленного рядом экспертов проекта Концепции кибербезопасности России [6]. В этом документе обоснованно подчеркивалось: «*В официальных российских документах в области информационной безопасности термин «кибербезопасность» не выделяется из объема понятия «информационная безопасность» и не используется отдельно. **В то же время в большинстве зарубежных стран он выделен в самостоятельную дефиницию***».

Напротив, в российских бизнес- и научной сферах использование терминов с корнем «кибер» росло синхронно с Западом. Здесь следует подчеркнуть ведущую роль профессора Д. П. Зегжды, по инициативе которого в 2020 году в Санкт-Петербургском политехническом университете был создан Институт кибербезопасности и защиты информации – первого в России вуза со словом «кибербезопасность» в официальном названии. Теория кибербезопасности киберфизических систем изложена в вышедшей недавно под его руководством фундаментальной монографии «Кибербезопасность цифровой индустрии» [8].

В 2020 году факультет «Информационные технологии» МТУСИ разделился на два факультета: «Информационные технологии» и «Кибернетика и информационная безопасность». Годом позднее Институт комплексной безопасности и специального приборостроения МИРЭА был переименован в Институт кибербезопасности и цифровых технологий. Кроме того, в ряде ФОИВ и системообразующих компаний России были созданы департаменты кибербезопасности, в частности департамент кибербезопасности ПАО «Сбербанк» стал первым подразделением в России, включившем в состав своего наименования слово «кибербезопасность».

Тем не менее, чтобы не противоречить действующему 149-ФЗ, кибербезопасность пока трактуется как составная и подчиненная часть информационной безопасности. В частности, департамент кибербезопасности ПАО «Сбербанк» де-факто занимается широким спектром направлений информационной безопасности (сферы его деятельности, согласно публичным данным: «защита IT-инфраструктуры Банка, противодействие кибермошенничеству, криптография, аутентификация и идентификация, защита персональных данных, защита банковских продуктов»). А в интервью газете «Коммерсант» от 23 июля 2020 года Д. П. Зегжда определил кибербезопасность как «самое передовое направление развития информационной безопасности». Тот же подход сохранен в монографии под его редакцией [8].

Размытость понятий цифровой терминологической экосистемы

Немецкому лингвисту Гуго Шухарду принадлежит меткая фраза: «Неясность терминологии так же опасна, как туман для мореплавателя». Это утверждение целиком относится к понятиям кодифицированных терминов, в неизменном виде перешедших в «цифровую парадигму» России из предыдущей «информационной парадигмы» (2000–2016 годы), и новых терминов, получающих все большее распространение в научном, техническом и бизнес-сообществах России, в том числе прозвучавших в ряде выступлений Президента РФ. Неполный список этих пересекающихся в понятиях терминов приведен в таблице.

В качестве примера неясности терминологии можно привести множество научных статей, в которых авторами делаются попытки найти различия между информационной безопасностью и кибербезопасностью, не выходя за рамки действующей парадигмы подчиненности и вторичности кибербезопасности по отношению к информационной безопасности.

Например, Н. Козлова в статье [9] приводит таблицу с семью различиями. Можно в качестве примера привести одно: «*Кибербезопасность предназначена для защиты киберпространства от кибератак, информационная безопасность занимается защитой данных от любых форм угроз*». Сразу возникает вопрос: если информационная безопасность занимается защитой данных от любых форм угроз, зачем нужна кибербезопасность?

Крайне фрагментарно определение А. Алпеева [10]: «*Кибербезопасность объекта – свойство объекта, характеризующее его внутренние*

Таблица. ***Термины цифровой экосистемы с пересекающимися понятиями***

Термины, кодифицированные на уровне федеральных законов, указов Президента РФ и постановлений Правительства РФ	Некодифицированные термины
• Технологический суверенитет	• Цифровой суверенитет • Цифровое государство • Цифровые границы • Киберсуверенитет • Кибериммунитет • Информационный суверенитет • Сетевой суверенитет • Цифровое общество
• Информационные технологии • Цифровая экономика • Автоматизированные системы управления • Информационные системы	• Цифровые технологии • Кибертехнологии • Цифровая индустрия • Индустрия 4.0 • Киберфизические системы
• Информационно-телекоммуникационная сеть • Критическая информационная инфраструктура • Информационная инфраструктура	• Киберпространство • Цифровое пространство • Цифровая среда • Информационное пространство
• Защита информации • Компьютерная безопасность • Компьютерная атака • Информационная безопасность	• Цифровая безопасность • Кибербезопасность • Кибератака • Киберпреступность • Информационная атака • Информационное противоборство • Информационная война • Кибервойна

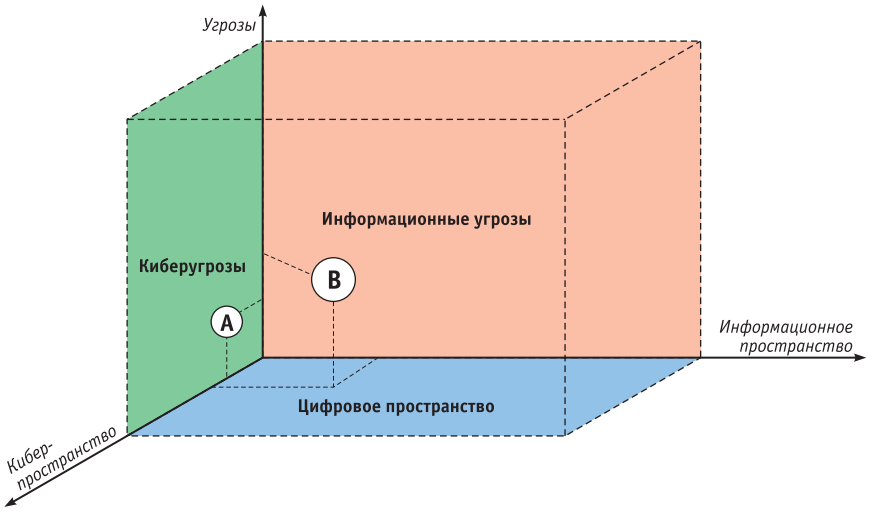


Рис. 3. ***Схематичное изображение цифрового информационного пространства***

возможности не быть причиной образования ущерба для внешней среды или ограничивать его величину допустимыми нормами».

Проект концепции стратегии кибербезопасности РФ 2013 года [6] дает определение киберпространства, по-прежнему концептуально смешивая его с информационным пространством: «***сфера деятельности в информационном*** *пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)».*

Л. Массель и Н. Воропай [11] справедливо отмечают: «*В России до сих пор нет однозначного понимания кибербезопасности. Часто ее считают синонимом информационной безопасности или ее части, в силу чего кибербезопасности не уделяется достаточного внимания*». Однако, в то же время, противореча самим себе, предлагают считать кибербезопасность результатом конвергенции безопасности приложений, информационной безопасности и сетевой безопасности.

Ряд других авторов, в частности, А. Ю. Баландин [20], Н. Ромашкина [22], А. Липатов [24] предлагают другие варианты, но все они не решают проблемы размытости кибер-информационных границ. Для примера можно привести цитату А. Баландина: «*Кибербезопасность представляется комплексной категорией, характеризующейся способностью системы противостоять угрозам, распространяющимся в цифровой среде*».

Основная причина такой концептуальной размытости, как уже отмечалось выше, видится в том, что продолжается инерция следования старой, датированной 70-ми годами прошлого века, американской концепции информационной безопасности в виде CIA-триады (см. рис. 2) со смешиванием в одном понятии «информационная безопасность» двух разных аспектов информации: антропоцентрической и функциональной (кибернетической), ***которые в сетецентрическую цифровую эпоху стали самостоятельными отдельными сущностями***.

Из всех авторов наиболее точно и системно исследовал проблемы, связанные с размытостью границ между информационной безопасностью и кибербезопасностью, А. С. Марков [22]. Настоящую статью отчасти можно считать развитием его идей.

Концепция демаркационной линии между информационной безопасностью и кибербезопасностью

26 марта 2021 года на совещании Совета безопасности РФ В. В. Путин сказал: «*Цифровое пространство становится площадкой жесткого информационного противоборства… и кибератак*». Таким образом, Президент РФ ввел в публичный оборот термин «цифровое пространство» и разделил в явном виде киберугрозы и информационные угрозы как отдельные сущности. Позднее, на расширенной коллегии ФСБ России 28 февраля 2023 года, в качестве отдельной сущности цифрового пространства было выделено информационное пространство: «*Значимая информация о наших системах управления, военных и правоохранительных структурах, предприятиях ОПК, критических технологиях и персональных данных должна быть надежно защищена. Необходимо и дальше повышать уровень защищенности* ***цифрового информационного пространства*** *России*».

В связи с вышеизложенным, слова Президента РФ необходимо понимать как новую систему координат, схематично изображенную на рис. 3.

Здесь цифровое информационное пространство определено как антропоцентрическая (воспринимаемая органами чувств и мозгом человека) информация, преобразованная в цифровую форму. Угрозы такому пространству необходимо классифицировать как информационные угрозы, а технологии защиты антропоцентрической информации – как информационную безопасность. Таким образом, функциональная (кибернетическая или машинная) информация (UEFI/BIOS и другое firmware, операционные системы, виртуальные машины, файловые системы, СУБД, различные встроенные СЗИ и антивирусное ПО, OSI-стэк сетевых протоколов), не являющаяся антропоцентрической, должна рассматриваться как кибернетическое пространство с присущими ему угрозами, которые классифицируются как киберугрозы.

Цифровое пространство является мета-пространством, образованным суперпозицией информационного и кибернетического пространств. Термин «суперпозиция» в рассматриваемом случае применен в значении операции, заключающейся в получении из данных двух функций f (информационное пространство) и g (киберпространство) новой функции

g(*f*) под названием «цифровое пространство». Такая же суперпозиция будет применима и в отношении пространств информационных и кибернетических угроз.

Как схематично показано на рис. 3, объект цифрового пространства в зависимости от своей сущности может иметь проекцию только в пространство киберугроз (киберфизические системы) или в оба пространства кибер- и информационных угроз (хранилища и базы данных, включая персональные, аналитические и финансовые системы, различные информационные бизнес-системы, телекоммуникационные сети, АПК «Безопасный город» субъектов РФ, АСУТП, цифровые СМИ, соцсети). Атака таких объектов из пространства киберугроз, например, на операционную систему, не обязательно нарушит целостность хранимой информации, но приведет к полному или частичному прекращению работы объекта и поддерживаемых им процессов экономики, госуправления или социально-культурных медиа.

В данной модели нет никакого противоречия с вышеприведенной цитатой Президента РФ на коллегии ФСБ России 28 февраля 2023 года. Его слова о защищенности информации, в частности, о наших критических технологиях, в информационном цифровом пространстве России как о зоне ответственности ФСБ России можно интерпретировать как проекцию данного объекта цифрового пространства на антропоцентрическое информационное пространство с точки зрения усиления его контрразведывательной защиты, которая не относится к сфере защиты киберпространства.

Новый взгляд на цифровой суверенитет России и концепцию его защиты

В своем выступлении на Совете Безопасности РФ 26 марта 2021 года Президент РФ еще раз подчеркнул, что «мы выступаем за незыблемость цифрового суверенитета».

Ряд авторов сам термин и концепцию цифрового суверенитета в целом считают отечественными, в частности, В. В. Бухарин [12], который, ссылаясь на Рунет, приписывает авторство термина Н. Н. Федотову, главному аналитику компании InfoWatch.

Однако на высшем уровне этот термин впервые прозвучал в Китае и был одной из инициатив Си Цзиньпина. Об этом говорится, в частности, в статьях Е. А. Михалевич [14] и Бай Яцзе [13], а также в мировой блогосфере 2015 года (статья BBC «Xi Jinping calls for „cyber sovereignty“»). На тот момент это касалось лишь суверенитета управления доступом граждан КНР в глобальный Интернет. Авторы [13] и [14] дают разный перевод прозвучавших из уст Си Цзиньпина китайских слов «ванло чжуцюань». Похоже, Е. А. Михалевич опиралась на англосаксонскую блогосферу, которая перевела их как cyber sovereignty, то есть киберсуверенитет, поэтому перевод Бай Яцзе можно считать более точным.

Бай Яцзе [13] отмечает бесспорное лидерство КНР в области цифрового суверенитета. Имея глубокую генетическую память о развязанных англосаксами в середине XIX века опиумных войнах и длительной утрате Китаем, вплоть до середины XX века, своего суверенитета, китайцы смогли одними из первых разглядеть скрытые «опиумные» угрозы в цифровом троянском коне от англосаксонских данайцев.

Однако, справедливости ради, необходимо отметить, что первым, кто пришел к идее цифрового суверенитета и разглядел скрытые угрозы англо-саксонской цифровой парадигмы, был французский бизнесмен Пьер Белланжер. В 2012 году в своей публикации [15] он определил цифровой суверенитет (souveraineté numérique) как *«контроль над сегодняшним днем и нашим общим будущим»*. Франко-канадец Stephane Couture [16] в своей статье прямо указывает, откуда исходят угрозы: *«В США цифровой суверенитет (или иное схожее по смыслу понятие) имеет крайне негативную коннотацию. В качестве примера можно привести публикацию Rand Corporation, критикующую концепцию «цифрового суверенитета» как нарушение прав человека»*.

В нашей стране термин «цифровой суверенитет» на государственном уровне начал употребляться с 2018 года после того, как в одном из публичных выступлений его произнес В. В. Путин.

В новой парадигме длительного противостояния России с коллективным Западом после начала СВО и открыто артикулируемых последним планов по полной ликвидации России как геополитического субъекта открывается новое измерение в вопросах угроз и вызовов нашей национальной безопасности и суверенитету. Отказ России и Китая быть управляемой частью Сети Запада и доктринальное закрепление примата своих суверенитетов рушит, ввиду критической значимости обеих стран для мировой экономики, всю их глобальную digital-парадигму, а потому является для Запада экзистенциальной угрозой.

С точки зрения американской концепции прокси-войн, подрыв нашего цифрового суверенитета представляется Западу наименее эскалационным видом агрессии, аналогичным прокси-войне на Украине и тотальной санкционной войне в отношении России. В случае решения Запада начать полномасштабную прямую вооруженную агрессию против России, реализуемую по стратегии мгновенного глобального удара (Global Prompt Strike), этот физический удар, очень вероятно, будет наноситься либо одновременно с глобальным мгновенным кибердаром, либо сразу после него. До начала агрессии, по уже известной западной практике, будет осуществлена операция по массированному социо-психологическому информационному удару по населению России через ее информационное пространство. Как известно, социо-психологическое информационное воздействие, диверсифицированное по всем слоям нашего общества, уже значительно возросло после 24 февраля 2022 года.

На совещании Совета Безопасности РФ 22 мая 2022 года Президент РФ потребовал «укреплять оборону отечественного цифрового пространства». Использование им слова «оборона» вместо «защита» вряд ли было случайным и свидетельствует, что уровень и характер угроз достиг критических размеров. Это дает допол-

нительные аргументы в пользу выделения информационной безопасности и кибербезопасности, образно говоря, в отдельные «рода войск», образующих новый вид «войск», который следует назвать «цифровой безопасностью» (рис. 4).

Цифровая безопасность как суперпозиция кибербезопасности и информационной безопасности

Термин «суперпозиция» в рассматриваемом случае применен в значении операции, заключающейся в получении из данных двух функций f (информационная безопасность) и g (кибербезопасность) новой функции $g(f)$ под названием «цифровая безопасность».

Термин «информационная безопасность» может употребляться исключительно в отношении антропоцентрической информации. Все, что относится к защите функциональной (кибернетической информации), не являющейся антропоцентрической, должно называться кибербезопасностью.

Становится все более очевидным, что принятый в 2006 году до начала цифровой эпохи 149-ФЗ и действующая «Доктрина информационной безопасности Российской Федерации» [18], утвержденная в декабре 2016 года, уже не отражают полный спектр современных геополитических вызовов.

В качестве подтверждения такого вывода можно привести тот факт, что в новых условиях уже потребовалось принятие отдельного подзаконного акта: «Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации», утвержденная Постановлением Правительства РФ № 4088р от 22 декабря 2022 года [17]. В этом документе термин «информационная безопасность» трактуется исключительно в социоантропоцентричном значении.

Также необходимо отметить, что в отличие от 187-ФЗ американская «The National Strategy to Secure Cyberspace» 2003 года распространяется на все национальное киберпространство, включая защиту объектов среднего и малого бизнеса и домохозяйств (в своем роде «гражданская кибероборона»). Эта проблема, в частности, поднимается в [20].

С учетом новых геополитических угроз представляется целесообразным:

- полный выход из старой западной парадигмы информационной безопасности 1977 года;
- принятие новой Доктрины цифровой безопасности России, отдельных федеральных законов и подзаконных актов о цифровой безопасности, информационной безопасности и кибербезопасности России;
- переработка программ обучения и подготовки специалистов в этих областях.

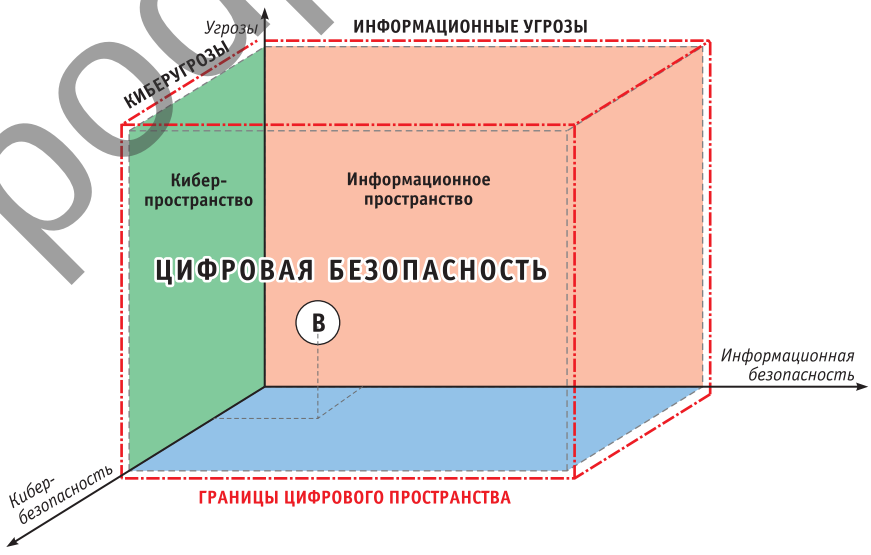


Рис. 4. ***Схематичная модель цифровой безопасности***

Замена термина и старой концепции «информационная безопасность» на новую концепцию «цифровая безопасность» позволит полностью гармонизировать по смыслам и понятиям всю корневую терминологию «Цифровое пространство» → Цифровые границы → Цифровой суверенитет → Цифровая безопасность → Цифровое государство → Цифровая экономика → Цифровое общество и т. д.».

Кибериммунитет и инфоиммунитет как ключевые направления развития технологий цифровой безопасности России

Среди множества пока неузаконенных в России терминов с корнем «кибер» одним из самых интересных является термин «кибериммунитет». Как термин «киберпространство» (cyberspace) пришел в доктринальные документы США из сферы андеграунд-фантастики, так и слово «кибериммунитет» было придумано дизайнерами игры Cyberpunk 2077, вдохновленными все той же книгой «Нейроман». С приходом в 2011 году цифровой парадигмы и развитием киберфизических систем оно стало западным техническим термином, быстро перенятым в России.

Технология кибериммунитета с точки зрения философии техники Эрнста Каппа является примером органопроекции, так же как и кибернетика Н. Винера была органопроекцией принципов самоорганизации сложных живых биологических систем на автоматизированные машинные системы. В этой связи современные сверхсложные и географически распределенные киберфизические системы, на основе которых строится цифровая экономика, должны сами защищать себя от угроз и атак, аналогично тому, как иммунитет защищает безопасность живого организма. Очевидно, что с возрастанием сложности и степени автоматизации киберфизических систем, увеличиваются, вплоть до катастрофических, и размеры ущерба в случае реализации в их отношении успешных кибератак. Технологии

атак также становятся предельно автоматизированными, поэтому человеческий фактор в обеспечении кибербезопасности становится самым уязвимым звеном.

Технологии и концепции кибериммунитета в настоящее время развиваются в России рядом компаний и экспертов, в частности С. А. Петренко [23], и являются одним из наиболее перспективных направлений развития кибербезопасности.

В рамках предлагаемой в статье новой концепции цифровой безопасности целесообразно экстраполировать понятие «иммунитет» и на информационное антропоцентрическое пространство России. Современные информационные атаки на основе искусственного интеллекта также становятся предельно автоматизированными. Технологии автоматизированного «инфоиммунитета» должны распознавать и отражать такие атаки максимально в автоматизированном режиме.

Концепция «инфоиммунитета» будет предложена в отдельной статье. В настоящей же работе проведено обоснование необходимости смены устаревших концепций информационного пространства и информационной безопасности новой концепцией цифрового пространства и концепцией цифровой безопасности. Предложена и обоснована четкая демаркационная линия между кибербезопасностью и информационной безопасностью, исключающая существующую размытость между этими понятиями. Предложена новая цифровая терминологическая экосистема, гармонизированная по понятиям терминов. Раскрыта ключевая особенность киберпространства цифровой экономики, заключающаяся в ее предельно сетецентрической архитектуре. ■

ЛИТЕРАТУРА

1. *Hilbert M. Digital Technology and Social Change: the Digital Transformation of Society from a Historical Perspective // Dialogues in Clinical Neuroscience. 2020. V. 22, № 2*
2. *Whisler T., Leavitt H. J. Management in the 1980's // Harvard Business Review. 1958 [Электронный ресурс]. – URL: https://hbr.org/1958/11/management-in-the-1980s/ (дата обращения: 12.10.2023).*
3. *Audit and Evaluation of Computer Security // 1977, National Bureau of Standards, U. S. Department of Commerce [Электронный ресурс]. – URL: https://www.nist.gov/publications/audit-and-evaluation-computer-security/ (дата обращения: 12.10.2023).*
4. *The National Strategy to Secure Cyberspace // 2003, U. S. Government via Department of Homeland Security [Электронный ресурс]. – URL: https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf (дата обращения: 12.10.2023).*
5. *Miller G., Nakashima E., Entous A. Obama's secret struggle to punish Russia for Putin's election // The Washington Post, June 23, 2017 [Электронный ресурс]. – URL: https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/ (дата обращения: 12.10.2023).*
6. *Концепция стратегии кибербезопасности Российской Федерации // Совет Федерации Федерального Собрания Российской Федерации, 2013 [Электронный ресурс]. – URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 16.10.2023).*
7. *Обновленная концепция конвенции Организации Объединенных Наций об обеспечении международной информационной безопасности // Совет Безопасности Российской Федерации 2023 [Электронный ресурс]. – URL: http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf (дата обращения: 12.10.2023).*
8. *Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам; [под ред. Д. П. Зегжды] // 2023. – М.: Горячая линия-Телеком. – 560 с.*
9. *Козлова Н. Ш., Довгаль В. А. Кибербезопасность и информационная безопасность: сходства и отличия // Вестник АГУ. – 2021. – Вып. 3 (286). – С. 88–97*
10. *Алпеев А. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. – 2014. – № 5 (8). – С. 39–42.*
11. *Массель Л., Воропай Н. Кибербезопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. – 2018. – № 4 (17). – С. 2–10.*
12. *Бухарин В. В. Компоненты цифрового суверенитета российской федерации как техническая основа информационной безопасности // Вестник МГИМО. – 2016. – № 6 (51). – С. 76–91.*
13. *Бай Яцзе, Зиновьева М. Практика цифрового суверенитета в России и КНР // Вестник Российского Совета по международным делам при МИД РФ, 25 мая 2023 [Электронный ресурс]. – URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (дата обращения: 18.10.2023).*
14. *Михалевич Е. А. Концепция киберсуверенитета Китайской Народной Республики: история развития и сущность // Вестник РУДН. Серия: Политология. – 2021. – Т. 23, № 2. – С. 254–264.*
15. *Bellanger P. De la Souveraineté Numérique» // Le Débat. 2012. № 170. P. 149–159.*
16. *Кутюр С., Тоупин С. Что означает понятие «суверенитет» в цифровом мире? // Вестник международных организаций. – 2020. – Т. 15, № 4. – С. 48–69.*
17. *Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации» (утв. Постановлением Правительства РФ № 4088р от 22 декабря 2022 года) // Правительство России, 2022 [Электронный ресурс]. – URL: http://government.ru/docs/all/145092/ (дата обращения: 16.10.2023).*
18. *Доктрина информационной безопасности Российской Федерации // Правительство России, 2016 [Электронный ресурс]. – URL: http://government.ru/docs/all/109306/ (дата обращения: 16.10.2023).*
19. *Баландин А. Ю. Кибербезопасность и информационная безопасность. Демаркация правовых категорий // Правовая политика и правовая жизнь. – 2023. – № 3. – С. 260–270.*
20. *Багдасарян Г. Ф., Кудряшов А. Л. Кибербезопасность и киберугрозы современного малого и среднего российского бизнеса // Вестник Евразийской науки. – 2023. – Т. s15, № 2 [Электронный ресурс]. – URL: https://esj.today/36favn223.html (дата обращения: 16.10.2023).*
21. *Ромашкина Н. П., Стефанович Д. В. Стратегические риски и проблемы кибербезопасности // Вопросы кибербезопасности. – 2020. – № 5 (39). – С. 77– 86.*
22. *Марков А. С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей // Вопросы кибербезопасности. – 2022. – № 1 (47). – С. 2–9.*
23. *Петренко С. А. Обзор методов иммунной защиты Индустрии 4.0 // Защита информации. Инсайд. – 2019. – № 5 (89). – С. 36–48.*
24. *Липатов А. Управление кибербезопасностью в нефтегазовой сфере России в условиях международных санкции // Московский экономический журнал. – 2023. – № 6 [Электронный ресурс]. – URL: https://qje.su/otraslevaya-i-regionalnaya-ekonomika/moskovskij-ekonomicheskij-zhurnal-6-2023-24/?print=print/ (дата обращения: 16.10.2023).*

О реализации программы импортозамещения в области телевидения

УДК 004.77; 004.056.5

В настоящее время отечественными операторами телевещания используется преимущественно зарубежное аппаратное и программное обеспечение (до 90 % каналов) для автоматизации процессов телепроизводства и эфирного вещания. Например, программное обеспечение Dalet Galaxy известной французской компании Dalet Digital Systems Media: News Wire – компьютерная система верстки новостей (Newsroom Computer System, NRCS), News Pro – система производства медиаконтента для новостей (Newsroom Production System, NRPS), News Library – система управления архивом медиа-контента, News Suite – комплексная система для обслуживания производственного процесса новостного вещания и др. Такая зависимость от зарубежных цифровых решений создала проблемную ситуацию. Уход иностранных производителей и прекращение технической поддержки в 2022–2024 годах в условиях беспрецедентного роста угроз информационной безопасности может привести к несанкционированному вмешательству в работу российских операторов. В настоящей статье рассмотрен ход реализации программ импортозамещения в области телевещания, возникающие при этом трудности, а также возможные пути их разрешения.

Ключевые слова: телевидение, оператор телевещания, телепроизводство, цифровые решения телепроизводства, импорт, импортозамещение, информационная безопасность, угрозы информационной безопасности, экономические санкции, экономическое развитие, цифровая экономика

Анна Сергеевна Петренко
a.petrenko2004@rambler.ru
Санкт-Петербургский государственный университет

Сергей Анатольевич Петренко, *доктор технических наук, профессор*
s.petrenko@rambler.ru
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Александр Дмитриевич Костюков, *кандидат юридических наук, старший научный сотрудник*
k-a777@yandex.ru
Севастопольский государственный университет

En On the Implementation of the Import Substitution Program in Television

A. S. Petrenko
a.petrenko2004@rambler.ru
St. Petersburg State University

S. A. Petrenko,
PhD (Eng., Grand Doctor), Full Professor
s.petrenko@rambler.ru
St. Petersburg State Electrotechnical University

A. D. Kostyukov,
PhD (Leg.)
k-a777@yandex.ru
Sevastopol State University

Currently, most domestic broadcast operatorsuse mainly foreign hardware and software to automate the processes of television production and broadcasting. Such dependence of Russian television broadcasting operators on foreign digital solutions has created a problematic situation. The cessation of technical support in 2022–2024 in conditions of growth of threats to information security may lead to interruptions and unauthorized interventions in the work of these operators. This article examines the progress of implementation of import substitution programs in the field of television broadcasting, the difficulties arising in this case, as well as possible ways to resolve them.

Keywords: television, television production, television broadcast operator, digital solutions for television production, import substitution, information security, threats

История вопроса

Современное развитие геополитической ситуации, усиление санкционного давления, распространение глобальных экономических вызовов обусловливают необходимость поиска возможностей для роста уровня экономического развития и достижения технологического суверенитета России, одной из которых является развитие импортозамещения. Здесь под *импортозамещением* понимается одна из стратегий государственной экономической политики, суть которой заключается в за-

мене на внутреннем рынке (как на потребительском, так и в производственном секторе) товаров иностранного производства на отечественные аналоги [1–9, 23].

Результаты научно-исследовательской деятельности по теме импортозамещения представлены в ряде трудов зарубежных и отечественных ученых. Так, теоретические основы импортозамещения зародились в трудах [34–37] и др., а российская практика представлена среди прочего в работах [1–9, 22–-24, 31, 32]. При этом одни отечественные исследователи сосредоточились на изучение роли санкций [1–9, 25–33], считая, что таковые предоставили хороший шанс инновационному развитию российской экономики, другие же больше внимания уделили проблеме обеспечения технологического суверенитета России [10–22, 38, 39].

Одной из первых стратегий государственной экономической политики стала «*Государственная программа развития сельского хозяйства и регулирования рынков сельскохозяйственной продукции, сырья и продовольствия*» (утверждена постановлением Правительства РФ от 14 июля 2012 года № 717)[1], направленная на снижение зависимости России от поставок продовольствия из-за рубежа. После введения в 2014 году первой волны экономических санкций Правительство РФ утвердило Государственную программу «*Развитие промышленности и повышение ее конкурентоспособности*» (утверждена постановлением Правительства от 15 апреля 2014 года № 328)[2]. Согласно этой программе, в 2015–2021 годах на проекты импортозамещения было выделено порядка 500 млрд руб. Это позволило довести долю отечественной составляющей в производстве товаров для гражданского потребления и перерабатывающей промышленности почти до 60 % (в агросекторе – еще больше). Однако в ряде критически важных отраслей экономики России подобные проблемы решены не были. По мнению аналитиков, этому помешала изначально заданная ориентированность проектов импортозамещения на экономическую обоснованность [1–9]. В результате ряд «нерентабельных» базовых производств, а их оказалось большинство, так и не получили финансирование.

В 2022 году (после начала СВО и введения более жестких санкций) государственный подход к импортозамещению изменился: последовавшие стратегии государственной экономической политики стали нацелены на обеспечение технологического суверенитета России. Согласно Проекту Федерального закона «О технологической политике в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» (подготовлен в сентябре 2023 года)[3], под *технологическим суверенитетом Российской Федерации* здесь понимается «*суверенитет, при котором обеспечено наличие под национальным контролем критических технологий, сквозных технологий и собственных линий разработки, жизненного цикла ключевых технических решений, созданы условия для обеспечения технологического паритета с иностранными государствами, а также самостоятельного производства высокотехнологичной продукции с применением указанных технологий*».

Сегодня к основным целям технологической политики Российской Федерации относятся:

- обеспечение технологического суверенитета Российской Федерации;
- обеспечение конкурентоспособности отечественной высокотехнологичной продукции и эффективности ее производства за счет разработки и внедрения технологических инноваций;
- ускоренная разработка и внедрение технологических инноваций для решения задач по повышению качества и уровня жизни граждан РФ и обеспечению безопасности и обороны государства.

Достижение перечисленных целей предполагает решение следующих задач:

1) определение приоритетных направлений технологического развития и целевых показателей достижения технологического суверенитета;

2) разработка и внедрение критических и сквозных технологий, формирование собственных линий разработки технологий и обеспечение контроля жизненного цикла ключевых технических решений со стороны российских юридических лиц;

3) установление специального правового режима разработки и использования критических и сквозных технологий, собственных линий разработки (далее – специальный правовой режим);

4) финансовое и налоговое стимулирование деятельности в сфере технологического развития в соответствии с приоритетными направлениями технологического развития;

5) разработка, производство и выведение на рынок различных видов высокотехнологичной продукции, созданных для обеспечения технологического суверенитета;

6) формирование долгосрочного спроса на высокотехнологичную продукцию, создаваемую для обеспечения технологического суверенитета;

7) создание благоприятных правовых условий для осуществления деятельности в сфере технологического развития, включая предоставление гарантий прав и законных интересов субъектов, осуществляющих формирование технологической политики Российской Федерации, и лиц, осуществляющих деятельность в сфере технологического развития;

8) создание благоприятных экономических и организационных условий для осуществления деятельности в сфере технологического развития;

9) организация международного сотрудничества в сфере технологического развития;

10) создание и развитие инфраструктуры для осуществления деятельности в сфере технологического развития, включая подготовку квалифицированных специалистов;

[1] *http://government.ru/rugovclassifier/815/events/.*
[2] *http://government.ru/rugovclassifier/862/events/.*
[3] *https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=239931#tzubX3UgHkkd0lwR2/.*

11) мониторинг эффективности технологической политики и оценка эффективности государственного стимулирования деятельности в сфере технологического развития (далее – государственное стимулирование), в том числе оценка уровня разработки и внедрения критических и сквозных технологий.

При этом различают следующие виды проектов технологического суверенитета:

- проекты, которые реализуются организациями и направлены на обеспечение серийного производства наиболее востребованной высокотехнологичной продукции с использованием критических технологий, разработку и внедрение отечественного программного обеспечения для критической информационной инфраструктуры на всех стадиях разработки, внедрения и развития технологических инноваций;
- *важнейшие проекты*, реализация которых имеет системное значение для функционирования экономики и решения социально-экономических задач Российской Федерации, обеспечения обороны и безопасности государства, достижения технологического паритета в области критических технологий с иностранными государствами, являющимися лидерами в соответствующей области.

Правительство РФ отобрало шесть приоритетных для импортозамещения секторов. Это базовые отрасли промышленности, энергетическая безопасность, обеспечение здравоохранения, транспортный сектор, обеспечение продовольственной безопасности, инфраструктура и жилищное строительство[4].

Программы импортозамещения цифровых решений

Летом 2022 года в рамках реализации национального проекта «Цифровая экономика РФ» по поручению Правительства РФ стали создаваться первые Индустриальные центры компетенций (ИЦК) по замещению зарубежных отраслевых цифровых продуктов и решений на отечественные технические решения в ключевых отраслях экономики[5]. Упомянутые центры образовались на принципах консорциумов из отечественных компаний (заказчиков, разработчиков и производителей цифровых решений), курировавших реализации значимых проектов импортозамещения промышленного (отраслевого) программного обеспечения, программно-аппаратных комплексов (ПАК), а также системного и прикладного ПО.

За год было создано 37 ИЦК и 13 центров компетенций разработки программного обеспечения под координацией 18 отраслевых комитетов. Задействовано 550 российских заказчиков, разработчиков и производителей решений. Для софинансирования расходов разработчиков были выделены гранты в размере 25,3 млрд руб. Проведена работа по уточнению 365 потребностей в отраслевых решениях, в том числе 85 – в общесистемном и прикладном ПО, проанализировано 1103 потребности в отраслевых решениях.

В результате этой масштабной работы были отобраны 197 проектов развития российских решений на 232 млрд руб. В 2023 году был подписан ряд соглашений с госкорпорациями для развития высокотехнологических направлений, более 20 особо значимых проектов были реализованы[6].

В 2023 году Минцифре России совместно с АНО «Центр компетенций по импортозамещению в сфере ИКТ», Российским фондом развития информационных технологий (РФРИТ) и фондом «Сколково» было поручено изучить проекты по разработке программного обеспечения, подготовленные ИЦК, на предмет их объединения и расширения функциональности конкретных решений. Это позволило укрупнить и отобрать проекты с «большим потенциалом тиражирования» в ключевых отраслях экономики[7].

В начале 2024 года фонд «Сколково» предоставил гранты на реализацию особо значимых проектов (ОЗП) в сфере телевидения[8], якорным заказчиком которых выступает Всероссийская государственная телевизионная и радиовещательная компания (ВГТРК) – крупнейший отечественный медиахолдинг [10, 29, 30]. Так, телеканал «Россия 1» является лидером на рынке национального вещания и считается одним из ведущих производителей телевизионных программ. Аудиторией телеканала являются 98,5 % населения России и более 50 млн телезрителей в странах СНГ и Балтии. С 2002 года ВГТРК ведет вещание международной версии канала – «РТР-Планета» –для жителей Европы, Ближнего Востока, Северной Африки и США. При этом медиахолдинг также входит в число крупнейших игроков российского Интернета: портал Вести.ru занимает третье место в рейтинге ведущих информационных сайтов Рунета, а его ежемесячная аудитория составляет около 17 млн уникальных пользователей. Кроме того, в онлайн-режиме ведут свое вещание основные телеканалы компании: «Россия 1», «Россия 2», «Россия 24», «РТР-Планета», а также радиостанции «Радио России», Радио «Маяк», «Вести FM» и др. [10, 29, 30].

Гранты фонда «Сколково» были выделены на создание доверенных и безопасных систем телевещания для телеканалов «Россия 1» и «Россия 24».

Первый проект направлен на доработку и внедрение системы автоматизации вещания и системы планирования и подготовки новостей в формате высокой четкости. Здесь разработчиком решения выступает

[4] *https://www.vedomosti.ru/economics/articles/2022/12/19/955864-minpromtorg-opredelil-prioriteti-gospodderzhki/.*
[5] *https://xn----dtbhaacat8bfloi8h.xn--p1ai/news/industrial-center-competition-jule-2022/.*
[6] *https://d-russia.ru/obshhie-itogi-raboty-industrialnyh-centrov-kompetencij-zampred-pravitelstva.html.*
[7] *http://government.ru/orders/selection/401/46589/.*
[8] *https://skolkovo-resident.ru/skolkovo-vydelil-granty-dlya-vgtrk/?ysclid=lsa9m9ljlr959054328/.*

«Технологии автоматизации вещания»[9].

Второй проект предполагает разработку и внедрение систем графического оформления эфира и виртуальных студий с привлечением компании «Кэрот Бродкаст»[10]. Согласно известным планам[11], будут доработаны подсистемы автоматизации телевещания и графического оформления эфира (табл. 1 и рис. 1–2). В том числе, основные подсистемы:

- видеозаписи;
- автоматизации вещания;
- контроля и управления;
- информационной безопасности;
- управления метаданными;
- новостной верстки, новостного вещания;
- файлового хранения и обработки;
- архивирования;
- мониторинга технологической инфраструктуры.

Также будет доработан ряд дополнительных подсистем:

- захвата и оцифровки медиаконтента;
- хранения и редактирования медиаконтента;
- подготовки и выдачи новостных выпусков в эфир;
- управления медиаконтентом;
- архивирования видеоматериалов;
- мониторинга и технического контроля и др.

Существенно, что для доработки систем телевещания и графического оформления эфира будут задействованы системное и прикладное ПО из единого реестра отечественного ПО[12], в том числе:

- языки программирования, трансляторы и фреймворки: *Qt 5, QT Creator, Golang, CMake, GCC, C++, Net6, LiteDB, OpenGL, JavaScript Vue, ffmpeg, LibXML, svn* и др.;
- операционные системы (ОС): *RED OC, Astra Linux, АЛЬТ 8* и др.;
- системы управления базами данных (СУБД): *Postgres Pro, Jatoba, Квант-Гибрид, Ред БД, ProximaDB, Arenadata PG*;
- комплекты разработчика (SDK): *vue, Qt 5*;
- интегрированные среды разработки (IDE): *QtCreator, QtDesigner, Qt Linguist*;
- средства для разработки интерфейсов OpenAPI: *XML, JSON, REST API* и пр.

Таблица. ***Типовые компоненты системы автоматизации телевещания***

Название подсистемы	Функциональное назначение
Подсистема видеосервера	Запись и воспроизведение видеоматериалов. Обеспечение приема и записи в медиафайлы цифровых компрессированных и некомпрессированных аудио- и видеопотоков. Воспроизведение медиафайлов и выдача цифровых компрессированных и некомпрессированных аудио- и видеопотоков, наложение графики, коммутация потоков медиаданных
Подсистема видеозаписи	Управление многоканальной синхронной и асинхронной записью аудио- и видеосигналов из различных источников. Предоставление многопользовательского доступа к управлению записью по расписанию или в ручном режиме
Подсистема автоматизации вещания	Формирование канального вещания телевизионных каналов. Обеспечение автоматического исполнения эфирных листов с управлением различным студийным оборудованием. Предоставление многопользовательского доступа к редактированию и управлению эфирными листами
Подсистема контроля и управления	Конфигурирование и обеспечение взаимодействия подсистем, авторизация пользователей, назначение прав и др. Обеспечение межсистемного взаимодействия, сбор логов и журналов, прием и рассылка уведомлений
Подсистема управления метаданными	Управление метаданными. Формирование структуры хранения метаданных. Предоставление многопользовательского доступа к метаданным
Подсистема новостной верстки	Создание и верстка сценариев новостных выпусков и событий. Обеспечение одновременной работы журналистов, корреспондентов, редакторов, шеф-редакторов и других участников производственного процесса создания информационных передач. Создание выпусков новостей и текстов сюжетов, связывание текстов с видеосюжетами и графическим оформлением
Подсистема новостного вещания	Автоматическая и ручная выдача в эфир заранее созданных эфирных новостных выпусков. Одновременное и последовательное воспроизведение эфирных материалов в студийных аппаратных по нескольким каналам вещательных серверов, управление студийным оборудованием. Контроль эфирного хронометража и синхронизации изменений эфирных листов видеосюжетов, графики, суфлеров
Подсистема файлового хранения и обработки	Управление медиафайлами. Обеспечение миграции файлового контента в ручном или автоматическом режимах, обработки звука, преобразования видео с возможностью смены формата, разрешения, кодека
Подсистема архивирования	Управление архивными материалами с использованием различных средств хранения. Многоуровневое хранение с интеллектуальной системой размещения и многокритериальным поиском
Подсистема мониторинга технологической инфраструктуры	Контроль состояния программного и аппаратного обеспечения комплексов в режиме реального времени. Мониторинг сетевого оборудования, серверных платформ, программных приложений и сервисов, рабочих мест пользователей и других объектов. Сохранение данных в течение заданного времени

При этом на замену классическим монолитным, 2- и 3-звенным программным архитектурам выбрана перспективная микросервисная архитектура, в том числе отечественные платформы контейнеризации

[9] *https://www.bramtech.ru/projects/regional-project-vgtrk-bram/?ysclid=lsa9tmr86p723594887/.*
[10] *https://www.carrot.software/.*
[11] *https://www.kommersant.ru/doc/5668324/.*
[12] *https://reestr.digital.gov.ru/.*

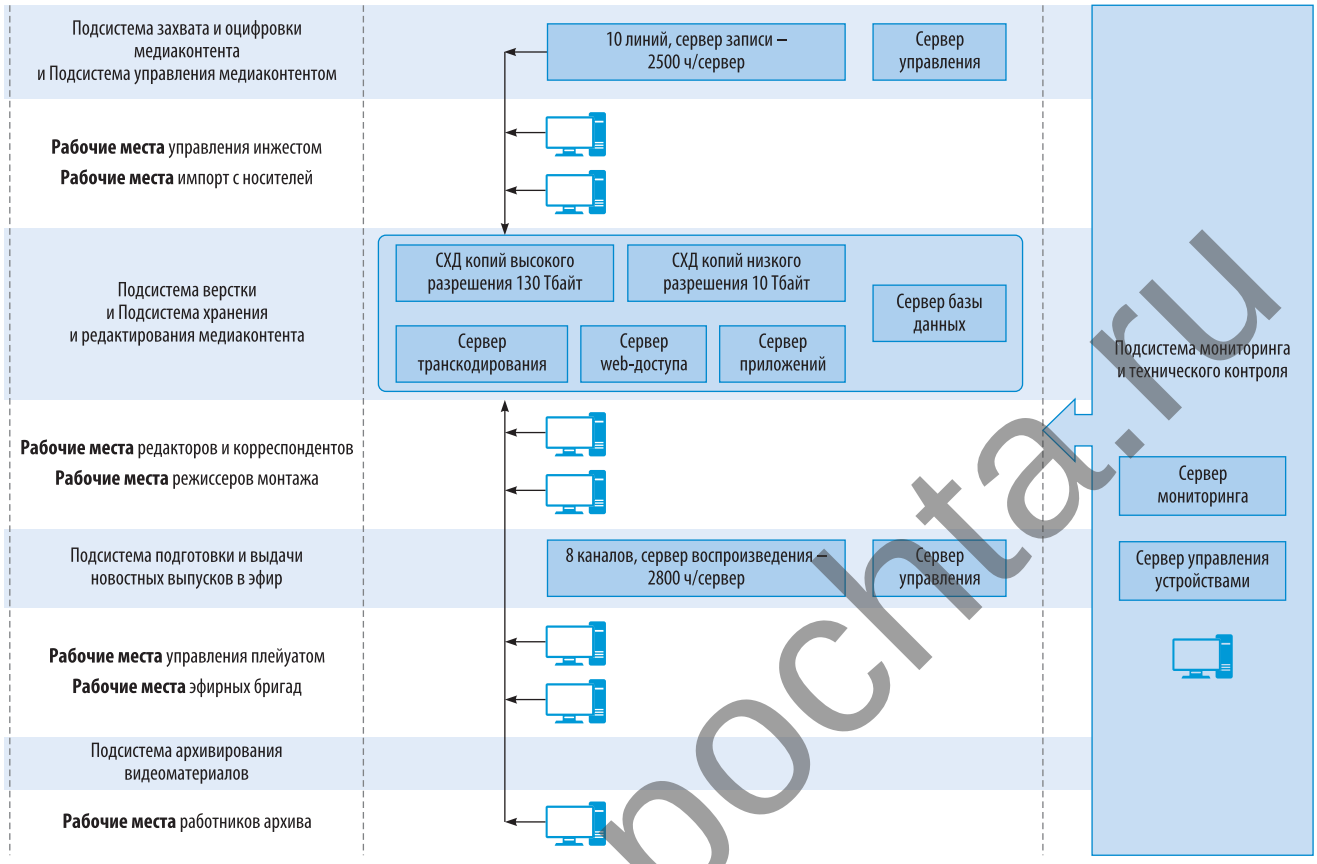


Рис. 1. ***Резервная подсистема программ «Вести» телеканала «Россия 1»***

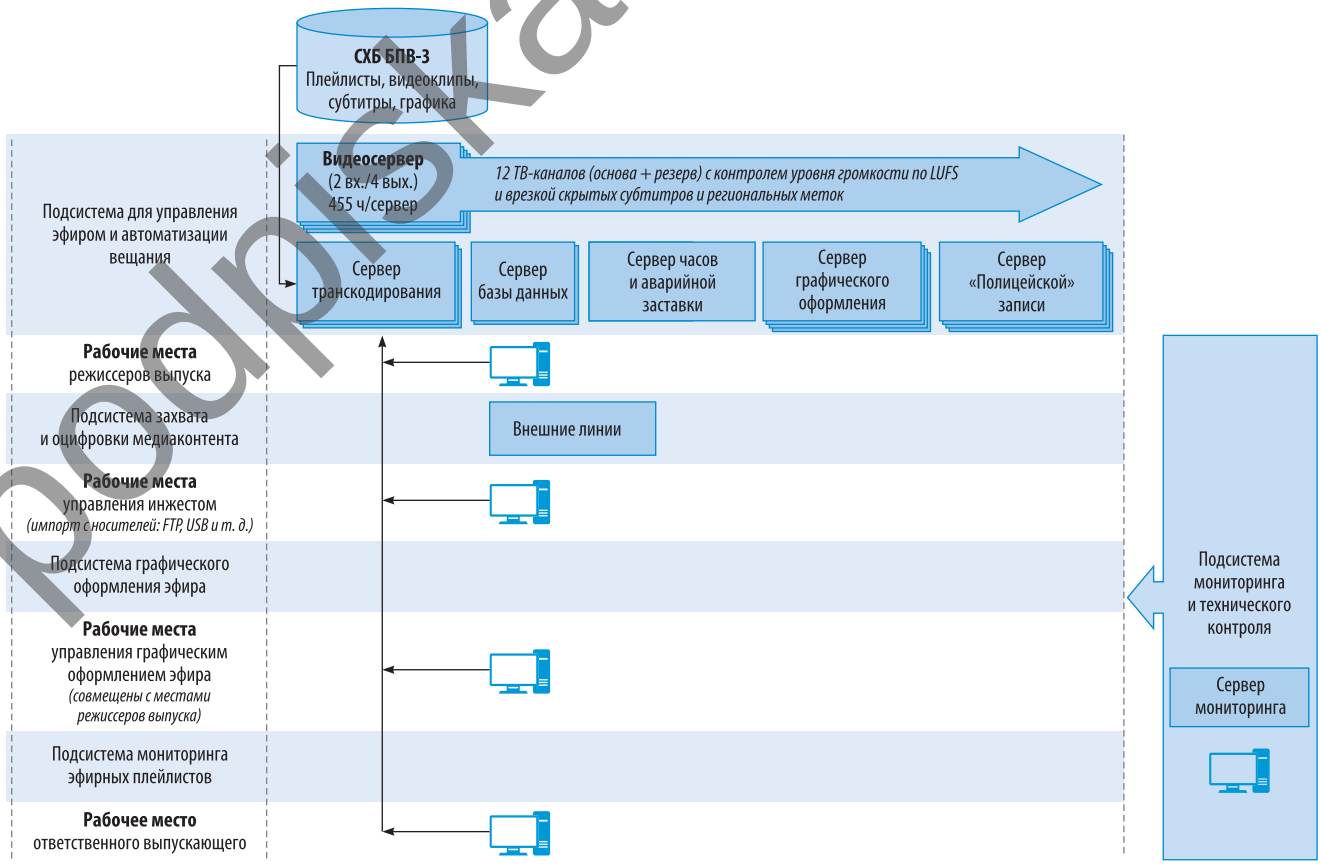


Рис. 2. ***Резервная подсистема телеканала «Россия 1»***

Kubernetes и управления контейнерной разработкой типа Deckhouse Kubernetes Platform[13].

Заключение

Основные направления развития отечественной отрасли телерадиовещания в Российской Федерации представлены в ряде программных документов [28–30]. В этих документах раскрыты основные цели и задачи государственной политики, расписаны основные этапы, ожидаемые сроки реализации и результаты. Так, например, в Концепции [13] одним из приоритетов является формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений. Для реализации названного приоритета запланировано проведение комплекса мероприятий, включающих:

- формирование безопасной информационной среды на основе популяризации информационных ресурсов, способствующих распространению традиционных российских духовно-нравственных ценностей;
- установление устойчивых культурных и образовательных связей с проживающими за рубежом соотечественниками, иностранными гражданами и лицами без гражданства, являющимися носителями русского языка, в том числе на основе информационных и коммуникационных технологий;
- принятие мер по эффективному использованию современных информационных платформ для распространения достоверной и качественной информации, прежде всего, российского производства;
- обеспечение насыщения рынка доступными, качественными и легальными медиапродуктами и видеосервисами российского производства;
- совершенствование механизмов законодательного регулирования распространения массовой информации, а также средств обеспечения доступа к информации, которые по многим признакам могут быть отнесены к средствам массовой информации, но не являются таковыми (интернет-телевидение, новостные агрегаторы, социальные сети, интернет-сайты, мессенджеры);
- принятие мер поддержки традиционных средств распространения информации (радио-, телевещание).

Программа импортозамещения в ВГТРК стартовала в 2015 году. Тогда же была предпринята первая попытка объединения российских производителей программно-аппаратного обеспечения в единый консорциум[14], в состав которого были приглашены ведущие отечественные компании: московские ЛЭС-ТВ, S-Pro Systems, StreamLabs, Digitab, Televiev, «Эпотел», BRAM Technologies, «Светоч-Сэмлайт», петербургская «Профитт», новосибирская «Софтлаб-НСК» и др. Для координации работы была создана дочерняя структура ВГТРК – АО «НПО «Перспектива»[15].

Благодаря государственной финансовой поддержке, за последнее десятилетие филиалы ВГТРК были выведены на кардинально новый уровень технического оснащения и производственного процесса. Все технологические участки переведены на цифровой формат обработки контента. Внедрены передовые методики новостной и программной автоматизации, единые для всех региональных компаний. Подавляющее большинство филиалов осуществляет съемку, обработку и хранение медиаконтента в формате высокой четкости (HD).

В 2023 году ВГТРК завершила работу над созданием крупнейшей в РФ наземной сети передачи телевизионных сигналов студийного качества, охватывающую 11 часовых поясов и объединившую 84 субъекта РФ. Сеть позволяет передавать сигналы отдельных телеканалов, пакеты телеканалов, ТВ-мультиплексы по принципу «каждый с каждым». Она также позволила ВГТРК оптимизировать логистику ТВ- и радиосигналов и гибко использовать ресурсы филиалов для формирования и распространения телерадиоканалов.

Новая наземная медиасеть ВГТРК стала альтернативой спутниковой доставке сигнала. Резервирование магистральных каналов и применение технологии программно-определяемых сетей (*Software-Defined Networking*, SDN) обеспечили высокую надежность доставки сигналов и открыли новые возможности для развития вещания в России. Партнерами сооружения сети выступили ПАО «Ростелеком» и его дочерняя компания АО «Синтерра Медиа»[16].

Успешная реализация профинансированных фондом «Сколково» проектов позволит доработать и внедрить новые и безопасные системы телевещания и графического оформления эфира на первых четырех пилотных телепроизводственных объектах ВГТРК «Россия 1» и «Россия 24»[17]. ■

ЛИТЕРАТУРА

1. Анимица Е. Г., Анимица П. Е., Глумов А. А. Импортозамещение в промышленном производстве региона: концептуально-теоретические и прикладные аспекты // Экономика региона. – 2015. – № 3 (43) . – С. 160–172. – DOI: 10.17059/2015-3-14.

2. Аракелян А. М., Воронцова Ю. В. Управление в сфере кино и телевидения: учеб. пос. – М.: ГУУ. – 2021. – 138 с.

3. Артемов В. В. Цифровые технологии в кино // Вестник ВГИК. – 2010. – Т. 2, № 1. – С. 132–138. – DOI: 10.17816/VGIK21132-138.

4. Атурин В. В. Антироссийские экономические санкции и проблемы импортозамещения в условиях современной международной конкуренции // Вестник евразийской науки. – 2019. – Т. 11, № 2. – С. 5–14.

[13] *https://www.kommersant.ru/doc/5668324/.*
[14] *https://tv-digest.ru/archive/id/46578/?ysclid=lsaaw7j8nf921767306/.*
[15] *https://tv-digest.ru/archive/id/46578/?ysclid=lsaaw7j8nf921767306/.*
[16] *https://www.content-review.com/articles/61787/.*
[17] *https://skolkovo-resident.ru/skolkovo-vydelil-granty-dlya-vgtrk/?ysclid=lsa9m9ljlr959054328/.*

5. Бодрунов С. Д. Теория и практика импортозамещения: уроки и проблемы: монография. – СПб.: ИНИР им. С. Ю. Витте. – 2015. – 171 с.

6. Борецкий Р. А. Беседы об истории телевидения. Лекции, прочитанные на факультете журналистики МГУ. – М.: Икар. – 2012. – 212 с.

7. Ваганова О. В. Влияние экономических санкций на инновационное развитие России // Научные ведомости Белгородского гос. ун-та. Серия: Экономика. Информатика. – 2019. – Т 46, № 1. – С. 21–30. – DOI: 10.18413/2411-3808-2019-46-1-21-30.

8. Гатиятулин Ш. Н., Орлов А. В. Проблемы импортозамещения в России и пути их разрешения // Форум. Серия: Гуманитарные и экономические науки. – 2022. – № 3 (26). – С. 8–12.

9. Глушич Н. Г., Лядова Е. В., Удалова Н. А. Основные противоречия реализации политики импортозамещения в экономике России // Журнал экономической теории. – 2017. – № 1. – С. 22–31.

10. Доклад о финансово-хозяйственной деятельности ФГУП «Всероссийская государственная телевизионная и радиовещательная компания» по итогам работы за 2020 год [Электронный ресурс]. – URL: https://digital.gov.ru/uploaded/files/vgtrk-doklad.pdf?utm_referrer=https %3a %2f %2fyandex.ru %2f/ (дата обращения: 03.12.2023).

11. Каравай И. Г., Салимжанова Д. Р. Принципы использования защитных инструментов во внешнеторговой деятельности России в рамках мирового рынка // Инновационная экономика и общество. – 2017. – № 1 (15). – С. 38–44.

12. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Д. П. Зегжды. – М.: Горячая линия-Телеком. – 2021. – 560 с.

13. Концепция развития телерадиовещания в Российской Федерации на 2020–2025 годы // Онлайн-журнал «Телеспутник» [Электронный ресурс]. – URL: https://telesputnik.ru/tvconcept/files/Concept.pdf (дата обращения: 03.12.2023).

14. Петренко А. С., Петренко С. А. О применении искусственного интеллекта в цифровом искусстве // Дистанционные образовательные технологии: сб. трудов VIII Междунар. науч.-практ. конф., Симферополь, 2023. – С. 349–352.

15. Петренко А. С., Петренко С. А. Классификация атак на модели данных генеративных изобразительных нейросетей // Дистанционные образовательные технологии: сб. трудов VIII Междунар. науч.-практ. конф., Симферополь, 2023. – С. 353–355.

16. Петренко А. С., Таран В. Н., Петренко С. А. Классификация атак на системы машинного обучения генеративных изобразительных нейросетей // Дистанционные образовательные технологии: сб. трудов VIII Междунар. науч.-практ. конф., Симферополь, 2023. – С. 356–359.

17. Петренко А. С., Таран В. Н., Петренко С. А. Киберустойчивость и безопасность генеративных изобразительных нейросетей // Дистанционные образовательные технологии: сб. трудов VIII Междунар. науч.-практ. конф., Симферополь, 2023. – С. 359–362.

18. Петренко А. С., Петренко С. А. Параметрический выбор киберустойчивой генеративной изобразительной нейросети // Дистанционные образовательные технологии: сб. трудов VIII Междунар. науч.-практ. конф.,Симферополь, 2023. – С. 363–366.

19. Петренко А. С., Петренко С. А., Ожиганова М. И. О киберустойчивости и безопасности изобразительных нейросетей // Защита информации. Инсайд. – 2023. – № 6 (114). – С. 50–54.

20. Петренко А. С., Петренко С. А., Костюков А. Д. Какие специалисты нужны отрасли информационной безопасности: DevSecOps-инженеры // Защита информации. Инсайд. – 2023. – № 6 (114). – С. 60–65.

21. Петренко С. А. Киберустойчивость цифровой экономики: науч.-поп. монография. – СПб.: Питер. – 2021. – 384 с.

22. Пичурин И. И., Блинов Д. В. Обеспечение импортозамещения после вступления России в ВТО: монография. – Екатеринбург: Изд-во УМЦУПИ. – 2014. – 144 с.

23. Попова И. Н., Сергеева Т. Л. Импортозамещение в современной России: проблемы и перспективы // Beneficium. – 2022. – № 2 (43). – С. 73–84. – DOI: 10.34680/BENEFICIUM.2022.2(43).

24. Пучков М. А., Алексунин В. А. Направления развития ВГТРК как зонтичного бренда // Гуманитарный акцент. – 2019. – № 3. – С. 38–45.

25. Селиверстов Ю. И., Чижова Е. Н. Западным санкциям Россия должна противопоставить импортозамещение и инновации // Вестник Алтайской академии экономики и права. – 2022. – № 5-3. – С. 442–449. – DOI: 10.17513/vaael.2231.

26. Симачев Ю. В., Федюнина А. А., Кузык М. Г. Российская промышленная политика в условиях трансформации системы мирового производства и жестких ограничений // Вопросы экономики. – 2022. – № 6. – С. 5–25. – DOI: 10.32609/0042-8736-2022-6-5-25.

27. Соколова О. Ю., Колотырин Е. А., Скворцова В. А. Импортозамещение как стратегия промышленной политики // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2017. – № 1 (41). – С. 130–139. – DOI: 10.21685/2072-3016-2017-1-13.

28. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 02.07.2021 № 400) // Совет Безопасности РФ [Электронный ресурс]. – URL: http://www.scrf.gov.ru/media/files/file/l4wGRPqJvETSkUTYmhepzRochb1j1jqh.pdf (дата обращения: 05.12.2023).

29. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (утв. Указом Президента РФ от 09.05.2017 № 203) // Президент России [Электронный ресурс]. – URL: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf (дата обращения: 05.12.2023)

30. Стратегия развития ВГТРК на период 2020–2024 гг. (утв. приказом Федерального агентства по печати и массовым коммуникациям (Роспечать) от 19.03.2020 № 71) // Кодексы online [Электронный ресурс]. – URL: https://gkrfkod.ru/zakonodatelstvo/prikaz-rospechati-ot-19032020-n-71/?ysclid=lsamkg0mbv949588972/ (дата обращения: 05.12.2023)

31. Строганов А. О., Жилина Л. Н. К истории вопроса об импортозамещении в России // Фундаментальные исследования. – 2015. – № 12–6. – С. 1278–1282.

32. Ушкалова Д. И., Никитина С. А. Влияние внешних факторов на экспорт и импорт России // Вестник Института экономики РАН. – 2019. – № 6. – С. 110–122. – DOI: 10.24411/2073-6487-2019-10074.

33. Шеметова М. Н. Костюм в кино. В Петербурге заявила о себе новая художественная школа // Вестник СПбГУ. Сер. 15. – 2015. – Вып. 4. – С. 137–159.

34. Bruton H. J. A Reconsideration of Import Substitution // Journal of Economic Literature. 1998. V. 36, № 2. P. 903–936.

35. Hirschman A. O. The Political Economy of Import-Substituting Industrialization in Latin America // The Quarterly Journal of Economics. 1986. V. 82, № 1. P. 1–32.

36. Westphal L. E. Industrial Policy in an Export Propelled Economy: Lessons from South Korea's Experience // Journal of Economics Perspectives. 1990. V. 4, № 3. P. 41–60.

37. Krueger A. Import Substitution Versus Export Promotion // Finance and Development. 1985. V. 22, № 2. P. 20–23.

38. Petrenko S. Cyber Security Innovation for the Digital Economy: A Case Study of the Russian Federation // River Publishers Series in Security and Digital Forensics. 2018. River Publishers. – 490 p.

39. Petrenko S. Cyber Resilience // River Publishers Series in Security and Digital Forensics. 2019. River Publishers. 1st ed. 2019. – 492 p.

Надзор 404: практика правоприменения запретов на вымогательство персональных данных

УДК 34.096

Рассмотрены практические результаты правоприменения запретов, направленных на противодействие незаконным попыткам получения персональных данных граждан со стороны некоторых коммерческих структур. Сделан вывод о ненадлежащем функционировании системы государственного надзора в рассматриваемой области.

Ключевые слова: персональные данные, защита прав потребителей, государственный надзор, законодательство Российской Федерации

Евгений Валерьевич Альтовский,
член правления
pr@ifap.ru
Общественное движение «Информация для всех»

Предисловие

1 сентября 2022 года вступили в силу поправки к Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных»[1] (далее – закон «О персональных данных») и закона РФ от 7 февраля 1992 года № 2300-I «О защите прав потребителей»[2] (далее – закон «О защите прав потребителей»), вменяющие в обязанность Роскомнадзору и Роспотребнадзору соответственно не допускать отказов в обслуживании потребителей, которые не захотели предоставлять свои персональные данные (ПДн) для целей, не связанных с предметом заключаемого ими договора. Например, банки отныне не могли отказать в заключении договора вклада, если вкладчик не хотел предоставлять свои ПДн аффилированной страховой компании для получения ее «специальных предложений», или соглашаться на их обработку банком для получения от него рекламы, которую правильнее было бы назвать спамом.

С тех пор ОД «Информация для всех» безуспешно пытается заста-

[1] *https://base.garant.ru/404993577/1cafb24d049dcd1e7707a22d98e9858f/.*
[2] *https://base.garant.ru/404561956/1cafb24d049dcd1e7707a22d98e9858f/.*

En

Supervision 404: the Law Enforcement Practice of Prohibitions on the Personal Data Extortion

E. V. Altovsky,
Board Member
pr@ifap.ru
NGO «Information for All»

The practical results of law enforcement in order to counteract illegal attempts to obtain personal data of citizens from some businesses are considered. The conclusion is made about the improper functioning of the system of state supervision in the consideration area.

Keywords: personal data, consumer protection, state supervision, legislation of the Russian Federation

вить указанные выше госорганы исполнять свои надзорные функции, обращаясь к ним с заявлениями о нарушении законодательства об обработке ПДн и о защите прав потребителей, которые остаются без удовлетворения, не рассматриваются по существу или вообще не рассматриваются, причем это происходит при попустительстве органов прокуратуры и судебной системы. Так прокуратура, обязанная надзирать за исполнением законов государственными органами, осуществляет «надзор» в форме пересылки жалоб на неисполнение законов таковыми самим нарушителям, а суды автоматически выносят решения в пользу госорганов, просто копируя мотивировочную часть решения из их отзывов на иск.

Далее мы покажем на конкретных примерах, как государственные гражданские служащие уклоняются от исполнения своих служебных обязанностей, как изобретательно они объясняют свое бездействие, как «обосновывают» свои решения «доводами», скопированными из отзывов на жалобы их фигурантов, и как надзорные органы потакают в этом государственным бездельникам, в свою очередь, уклоняясь от исполнения служебных обязанностей.

Наша разнообразная, хоть и ограниченная практика позволяет сделать обобщение: разработанные правительством страны, принятые ее парламентом и подписанные президентом поправки к законодательству, направленные на противодействие вымогательству у граждан их персональных данных, на этапе правоприменения сталкиваются с ленью, некомпетентностью и откровенным саботажем чиновников, демонстративно отказывающихся выполнять свою работу.

1. Оценка правовых норм

1.1. Закон «О персональных данных»

Часть 3 статьи 11^3 закона «О персональных данных» гласит: *оператор не вправе отказывать в обслуживании в случае отказа субъекта персональных данных предоставить биометрические персональные данные и (или) дать согласие на обработку персональных данных, если в соответствии с федеральным законом получение оператором согласия на обработку персональных данных не является обязательным.*

Формулировка данной правовой нормы представляется нам в целом адекватной поставленной задаче за исключением диспозиции «отказывать в обслуживании», которая предусматривает лишь случаи оказания услуг, но не выполнения работ или купли-продажи.

Более значимой проблемой рассматриваемой нормы представляется отсутствие в Кодексе Российской Федерации об административных правонарушениях (КоАП РФ) корреспондирующей нормы, предусматривающей соответствующую санкцию. Полномочия ФОИВ, осуществляющего функции по контролю (надзору) за соответствием обработки ПДн требованиям законодательства (Роскомнадзора) предусматривают в данном случае лишь вынесение предписания об устранении выявленных нарушений по результатам проверки.

Вместе с тем, в силу постановления Правительства Российской Федерации от 10 марта 2022 года № 336 «Об особенностях организации и осуществления государственного контроля (надзора), муниципального контроля»[4] (далее – Постановление № 336), в 2022–2023 годах внеплановые контрольные (надзорные) мероприятия проводятся надзорным органом лишь при наличии экстраординарных оснований, таких как причинение или непосредственная угроза причинения вреда жизни или здоровью граждан, обороне страны или безопасности государства и т. п.

Очевидно, что в общем случае отказ в обслуживании в случае нежелания субъекта ПДн дать согласие на их обработку не причиняет такого вреда и не создает угроз его причинения, вследствие чего рассматриваемую норму в настоящий момент следует считать «мертвой». Тем не менее, известная практика правоприменения данной нормы показывает, что Роскомнадзор не намерен применять ее в принципе, выдвигая абсурдные причины и поводы для уклонения от исполнения надзорных функций (что будет показано далее).

1.2. Закон «О защите прав потребителей»

Часть 4 статьи 16^5 закона «О защите прав потребителей» гласит: *продавец (исполнитель, владелец агрегатора) не вправе отказывать потребителю в заключении, исполнении, изменении или расторжении договора с потребителем в связи с отказом потребителя предоставить персональные данные, за исключением случаев, если обязанность предоставления таких данных предусмотрена законодательством Российской Федерации или непосредственно связана с исполнением договора с потребителем.*

Оставим за скобками уместность включения правовой нормы, которая регулирует оборот ПДн, в законодательство о защите прав потребителей, тем более при наличии аналогичной нормы в законе «О персональных данных». Отметим другое: формулировка первого абзаца правовой нормы представляется неадекватной поставленной задаче, поскольку оперирует терминологией, отличной от используемой в законе «О персональных данных». Кроме того, ее диспозиция предусматривает лишь случаи предоставления ПДн (*«в связи с отказом потребителя предоставить персональные данные»*). Такая формулировка позволяет вывести из-под действия рассматриваемой нормы случаи, когда оператор (в терминологии рассматриваемой нормы – продавец, исполнитель, владелец агрегатора) уже располагает персональными данными субъекта (в терминологии рассматриваемой нормы – потребителя) и понуждает того к предостав-

[3] *https://base.garant.ru/12148567/9d78f2e21a0e8d6e5a75ac4e4a939832/.*
[4] *https://base.garant.ru/403681894/.*
[5] *https://base.garant.ru/10106035/7a58987b486424ad79b62aa427dab1df/.*

лению не самих ПДн, а лишь согласия на их обработку в целях, не связанных с исполнением договора между ними и не предусмотренных законодательством.

В качестве примера можно привести случай, когда оператор заключает договор с субъектом на условиях, соответствующих рассматриваемой норме, однако затем понуждает субъекта принять изменения или дополнения к заключенному договору, уже не соответствующие ей, отказываясь в противном случае от исполнения заключенного договора или его части, искусственно затрудняя исполнение договора для субъекта и т. п. (реальный пример таких действий приведен в разделе 2.1). Таким образом, предоставление самих персональных данных происходит в соответствии с законом, тогда как последующее вымогательство согласия на их обработку в целях, не связанных с исполнением договора и не предусмотренных законодательством, остается не урегулировано рассматриваемой нормой.

Еще на этапе рассмотрения соответствующего законопроекта парламентом на недостаток проектируемой нормы указывалось ответственным комитетам Госдумы РФ: по экономической политике, промышленности, инновационному развитию и по промышленности и торговле, а также Правому управлению Госдумы РФ. Одновременно предлагалась редакция первого абзаца, устраняющая этот недостаток, которая не была принята во внимание законодателем: Продавец (исполнитель, владелец агрегатора) не вправе отказывать в заключении, исполнении, изменении или расторжении договора в связи с отказом потребителя предоставить согласие на обработку своих персональных данных, за исключением случаев, когда обязанность предоставления такого согласия предусмотрена законодательством Российской Федерации или непосредственно связана с исполнением договора с потребителем.

Частью 7 статьи 14.8[6] КоАП РФ установлена санкция за *отказ в заключении, исполнении, изменении или расторжении договора с потребителем в связи с отказом потребителя предоставить персональные данные, за исключением случаев, если предоставление персональных данных является обязательным в соответствии с федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами или непосредственно связано с исполнением договора с потребителем.*

В последние годы надзорные органы часто уклоняются от возбуждения производства по делу об административном правонарушении со ссылкой на Постановление № 336. Такая практика была признана незаконной судами[7], указавшими, что ч. 1 ст. 24.5 КоАП РФ установлен закрытый список обстоятельств, наличие которых исключает начало производства по делу об административном правонарушении, среди которых отсутствуют установленные правительством страны ограничения. Несмотря на это, Роскомнадзор активно пользуется незаконным предлогом, чтобы уклониться от надзора за соблюдением законодательства об обработке ПДн, тогда как Роспотребнадзору, и мы покажем это в статье, не требуется даже предлог, чтобы уклониться от работы.

2. Опыт правоприменения закона «О персональных данных»

2.1. «Личный кабинет» абонента ПАО «Вымпелком»

Экспозиция: *физическое лицо – абонент ПАО «Вымпелком», пользователь личного кабинета (ЛК) абонента на сайте оператора (my.beeline.ru) при очередной авторизации в ЛК столкнулся с требованием принять «оферту»[8]; в случае отказа абоненту не предоставлялся доступ в ЛК.*

Согласно «оферте» (мы ставим это слово в кавычки, поскольку оферта означает предложение, а не ультиматум) от абонента требовалось согласие на обработку его ПДн в целях распространения рекламы (в том числе от любых третьих лиц) и передачу ПДн третьему лицу. При этом указывалось, что абонент сможет отозвать согласие на обработку своих персональных данных в целях, непосредственно не связанных с исполнением договора связи.

1 сентября 2022 года абонент отказался соглашаться с требованиями «оферты» и подал заявление о нарушении законодательства об обработке ПДн в Управление Роскомнадзора по Центральному федеральному округу (ЦФО), в котором просил:

- вынести ПАО «Вымпелком» предписание о приведении условий «оферты» в соответствие с требованиями законодательства, регулирующего порядок обработки персональных данных;
- возбудить в отношении ПАО «Вымпелком» дело об административном правонарушении, предусмотренном ст. 13.11 КоАП РФ;
- признать заявителя потерпевшим по делу об административном правонарушении.

Письмом № 107203-02-11/77 от 28 октября 2022 года заявителю было отказано по всем пунктам. Вместе с тем сообщалось, что «в ПАО «Вымпелком» направлено письмо об изменении требований (видимо, «оферты»), и приведении их в соответствие с п. 5 ч. 1 ст. 6 Закона (о персональных данных) и необходимости их неукоснительного соблюдения». Указанный пункт закона содержит бланкетную норму о необходимости обработки персональных данных операторами в соответствии с законом и в целях, не выходящих за рамки исполнения договора между оператором ПДн и их субъектом.

Согласно приложенному Определению об отказе в возбуждении

[6] *https://www.consultant.ru/document/cons_doc_LAW_34661/59f86440655bf2aec393fd031c5a4bc13cfcdc17/.*

[7] *См., например, постановление Одиннадцатого арбитражного апелляционного суда по делу № А65-31134/2022: https://sudact.ru/arbitral/doc/sqW6ON4QK4U4/.*

[8] *С полными текстами всех упомянутых в настоящей статье документов, включая переписку с надзорными органами, можно ознакомиться в соответствующем докладе ОД «Информация для всех»: https://ifap.ru/library/book682.pdf.*

дела об административном правонарушении, данное решение было вынесено в связи с тем, что из заявления не очевидно, что ПАО «Вымпелком» уже фактически ведет обработку персональных данных с нарушением применимых требований законодательства.

С учетом ранее изложенного, в том числе приведенной оценки правовой нормы закона «О персональных данных», полагаем, что в данном случае Роскомнадзором были приняты все доступные ему меры реагирования. Однако в дальнейшем Управление отказалось принимать меры по данному эпизоду и фактически отказалось рассматривать аналогичное заявление, что, возможно, связано со сменой руководителя профильного направления Управления.

В результате упомянутого требования Управления, содержание «оферты» было частично изменено. В частности, из нее было исключено требование согласиться на получение рекламы, однако ряд других спорных требований исключен не был, в том числе требование согласиться на передачу ПДн третьему лицу, в связи с чем заявитель подал новое заявление в Управление.

Одновременно внимание Управления обращалось на содержащиеся в действиях ПАО «Вымпелком» признаки правонарушений, предусмотренных ст. 19.5 и ст. 19.7 КоАП РФ, предусматривающих ответственность за представление в госорган информации в искаженном виде и за невыполнение в установленный срок предписания органа, осуществляющего госнадзор, об устранении нарушений законодательства.

На указанное заявление поступил ответ Управления, который не соответствовал предмету жалобы и игнорировал указания на признаки административных правонарушений. Данный ответ был обжалован заявителем, на что последовало вынесение Определения об отказе в возбуждении дела об административном правонарушении, которое также не соответствовало предмету жалобы и игнорировало указания на признаки правонарушения, предусмотренного ст. 19.5 КоАП РФ.

Вместе с тем, указанное определение содержало любопытный фрагмент: *«В своем ответе ПАО „ВымпелКом“ сообщает, что <…> доводы Заявителя не соответствуют действительности, ни старый, ни новый текст Оферты никогда не содержали следующие условия: „Также абонент выражает согласие на направление сообщений рекламного и/или информационного характера по любым каналам коммуникаций, включая рассылку по сети подвижной связи коротких текстовых сообщений (SMS), направление push- сообщений, демонстрацию баннерной, контекстной и иной рекламы в сети Интернет и социальных сетях, на публично доступных видеоустройствах/электронных мониторах, а также организацию Оператором канала коммуникации между Партнерами по телефонным номерам, пользователем которых является Заявитель“».*

Дело в том, что заявитель никогда не упоминал в своих заявлениях положение оферты, которое было выделено кавычками как цитата, и оно не входило в текст оферты ни в одной из ее редакций, ставших предметом жалоб. По всей видимости, либо ПАО «Вымпелком», либо Управление Роскомнадзора по ЦФО скопировало этот фрагмент «возражения» заявителю из какого-то другого текста, не относящегося к рассматриваемому делу. Как бы то ни было, в основу определения об отказе в возбуждении дела об административном правонарушении был среди прочего положен некий случайный текст, не имеющий отношения к рассматриваемому вопросу. Итогом правоприменения стало частичное изменение текста «оферты» ПАО «Вымпелком», навязываемой пользователям личного кабинета абонента и исключение из него требования согласиться на получение рекламы. Требование согласиться на передачу ПДн третьему лицу в тексте «оферты» сохранилось.

2.2. Договор о вкладе с ПАО «Сбербанк»

Экспозиция: *физическое лицо – клиент ПАО «Сбербанк» – имел намерение заключить договор срочного вклада (депозита). Однако п. 11 ст. 2 данного договора содержал требование согласиться на получение рекламы. При этом в том же пункте указывалось, что данное согласие может быть затем отозвано клиентом.*

18 февраля 2023 года клиент отказался заключать договор в указанной редакции и подал заявление о нарушении законодательства об обработке ПДн в Управление Роскомнадзора по Центральному федеральному округу, в котором (с учетом ранее полученных от Управления разъяснений) просил вынести ПАО «Сбербанк» предписание об исключении из договора банковского вклада п. 11 ст. 2.

Ответным письмом заявителю было полностью в этом отказано, поскольку *«субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе», а текст договора предоставляет клиенту банка «самостоятельно принять решение о предоставлении своих персональных данных»*.

В связи с этой позицией Управления, заявитель обратился к Начальнику Управления по защите прав субъектов персональных данных Роскомнадзора Ю. Е. Контемирову с запросом официального разъяснения: в каком случае Роскомнадзор будет требовать от операторов ПДн исполнения ч. 3 ст. 11 закона «О персональных данных», если в современной деловой практике субъекта ПДн, как правило, не заставляют их предоставлять угрозами или силой, следовательно, всегда можно считать, что если субъект дает согласие на обработку своих ПДн, то делает это *«свободно, своей волей и в своем интересе»*?

В ответном письме указанное должностное лицо сообщило следующее (не дав ответа по сути поставленного вопроса):

- положение договора о рассылке рекламы является его *«неотъемлемым условием и подлежит обязательному исполнению»*;
- запрет, установленный ч. 3 ст. 11 закона *«О персональных данных»*, *«относится исключительно к обработке биометрических персональных данных. В отношении осталь-*

ных категорий персональных данных указанное требование не распространяется».

В повторном запросе, направленном с целью разъяснения вышеприведенных формулировок, внимание должностного лица обращалось на следующие факты:

- в самом п. 11 ст. 2 договора о вкладе указывается, что согласие на получение рекламы «*может быть отозвано Вкладчиком в любой момент*», следовательно, утверждение, будто данный пункт является неотъемлемым условием и подлежит обязательному исполнению, ошибочно;
- ч. 3 ст. 11 закона оперирует обоими понятиями – «*биометрические персональные данные*» и «*персональные данные*», однозначно устанавливая запрет на вымогательство любых ПДн, а не только биометрических; кроме того, данная трактовка также явно прописана в пояснительной записке[9] к соответствующему законопроекту следующим образом: «*устанавливается прямой запрет Операторам на отказ гражданам в оказании услуг при отказе предоставить свои персональные данные (в том числе биометрические), если такое предоставление не является обязательным*».

Указанный запрос в нарушение порядка рассмотрения обращений граждан остался без ответа. В то же время заявителем было получено письмо от вышестоящего должностного лица в связи с поступлением в Роскомнадзор депутатского запроса Ольги Тимофеевой (подробнее см. раздел «Опыт правоприменения нормы закона „О защите конкуренции“»), где сообщалось, что рассматриваемое положение договора «*осуществляется в рамках заключения и исполнения Договора и, как следствие, подпадает под действие п. 5 ч. 1 ст. 6 Федерального закона 152-ФЗ и не требует получения согласия со стороны вкладчика*». Таким образом, по мнению заместителя главы Роскомнадзора – куратора Управления по защите прав субъектов персональных данных М. Э. Вагнера, обработка персональных данных в целях рассылки рекламы необходима для исполнения договора банковского вклада и потому не требует согласия вкладчика, хотя даже сам банк в договоре утверждает прямо противоположное.

Также в указанном письме воспроизводилось ложное утверждение, что запрет вымогательства касается только биометрических ПДн, а субъектам «обычных» ПДн рекомендовалось обращаться за защитой своих прав в Роспотребнадзор.

Итогом правоприменения стало закрепление позиции надзорного органа (Роскомнадзора), заключающейся в следующем: если субъект персональных данных не согласен с их обработкой в целях, не связанных с исполнением договора между ним и оператором ПДн, он может отказаться от заключения такого договора, оспорить его в суде или обратиться в Роспотребнадзор. При этом Роскомнадзор не видит оснований для реагирования, если дело касается «обычных», а не биометрических ПДн.

3. Опыт правоприменения закона «О защите прав потребителей»

3.1. «Личный кабинет» абонента ПАО «Вымпелком»

Экспозиция: *см. раздел 2.1.*

1 сентября 2022 года абонент отказался принимать «оферту» в указанной редакции и подал заявление о нарушении законодательства о защите прав потребителей в Управление Роспотребнадзора по городу Москве, в котором просил:

- вынести ПАО «Вымпелком» предписание о приведении условий «оферты» в соответствие с требованиями законодательства о защите прав потребителей;
- возбудить в отношении ПАО «Вымпелком» дело об административном правонарушении, предусмотренном ч. 7 ст. 14.8 КоАП РФ;
- признать заявителя потерпевшим по делу об административном правонарушении.

Определением об отказе в возбуждении дела об административном правонарушении заявителю было отказано по всем пунктам. В качестве обоснования своей позиции Роспотребнадзор сообщил: «*Личный кабинет является **дополнительной** услугой, которую оператор связи предоставляет абонентам для удобства получения информации по договору на оказание услуг связи. Абонент вправе не использовать личный кабинет, при этом оператор связи продолжает предоставлять абоненту услуги по договору на оказание услуг связи*».

Процитированный фрагмент определения был целиком скопирован Роспотребнадзором из отзыва ПАО «Вымпелком» на жалобу. Данное определение было обжаловано у вышестоящего должностного лица, которое вынесло аналогичное решение со ссылкой на все ту же «дополнительную» услугу, которой абонент вправе не пользоваться, если не согласен с условиями ее оказания.

Указанное решение, в свою очередь, было обжаловано у вышестоящего должностного лица, однако Управление Роспотребнадзора по городу Москве без ведома заявителя переслало жалобу в Останкинский районный суд города Москвы, который принял жалобу в территориальное управление Роспотребнадзора в качестве искового заявления и рассмотрел дело об административном правонарушении при вызове «истца» в качестве «привлекаемого лица»[10].

Решением по делу суд полностью отказал в удовлетворении исковой жалобы, аргументировав свою позицию ссылкой на все ту же «дополнительность» услуги и свободу договора. Попытка обжаловать решение суда в апелляционной инстанции закончилась возвратом апелляционной жалобы по причине того, что поданная в электронном виде через ГАС «Правосудие» жалоба якобы поступила в суд апелляционной

[9] *См. карточку законопроекта на сайте Госдумы: https://sozd.duma.gov.ru/bill/101234-8/.*

[10] *См. материалы дела № 12-112/2023 (12-5187/2022), https://mos-gorsud.ru/rs/ostankinskij/services/cases/appeal-admin/details/c99f69f0-7573-11ed-95a5-9302fbeb6235/.*

инстанции по электронной почте и не содержала подписи заявителя. По данному факту было направлено заявление председателю суда первой инстанции об устранении процессуальных нарушений, допущенных судом, которое было проигнорировано.

3.2. Договор о вкладе с ПАО «Сбербанк»

Экспозиция: *см. раздел 2.2.*

18 февраля 2023 года клиент отказался заключать договор в указанной редакции и подал заявление о нарушении законодательства о защите прав потребителей в Управление Роспотребнадзора по городу Москве, в котором просил:

- вынести ПАО «Сбербанк» предписание об исключении из договора пункта, предусматривающего безусловное согласие вкладчика на получение рекламных и информационных сообщений;
- возбудить в отношении ПАО «Сбербанк» дело об административном правонарушении, предусмотренном ч. 7 ст. 14.8 КоАП РФ;
- признать заявителя потерпевшим по делу об административном правонарушении.

Определением об отказе в возбуждении дела об административном правонарушении заявителю было отказано по всем пунктам по той причине, что «*правовой анализ приложенного [к заявлению] документированного материала не позволил установить наличие в действиях юридического лица вышеуказанного состава административного правонарушения*». При этом никакого обоснования такого вывода либо оценки доводам заявителя на трех страницах бюрократического словоблудия дано не было.

На указанное определение была подана жалоба в Прокуратуру г. Москвы с указанием на факт уклонения должностным лицом Роспотребнадзора от возбуждения дела об административном правонарушении, которая вопреки требованиям, установленным ч. 6 ст. 8[11] Федерального закона от 2 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», а именно, запрета направлять жалобу на рассмотрение в государственный орган, бездействие которого обжалуется, тем не менее была переслана на рассмотрение в Роспотребнадзор, который отказался ее рассматривать под предлогом пропуска срока на обжалование.

3.3. Запрос информации у ПАО «Сбербанк»

Экспозиция: *клиент ПАО «Сбербанк» запросил у этого учреждения информацию о причинах и правовых основаниях, определяющих невозможность заключения договора о вкладе без предоставления персональных данных для целей, не связанных с исполнением договора.*

Согласно ч. 4 ст. 16 закона «О защите прав потребителей», при предъявлении потребителем подобного требования, «Сбербанк» был обязан предоставить запрошенную информацию в течение 7 дней, но не сделал этого. В этой связи клиент обратился в Управление Роспотребнадзора по городу Москве с просьбой провести проверку соблюдения ПАО «Сбербанк» законности при рассмотрении указанного запроса информации. По результатам рассмотрения жалобы Роспотребнадзор отказал в принятии мер со ссылкой на ст. 9 Федерального закона от 2 декабря 1990 года № 395-1 «О банках и банковской деятельности», согласно которой органы исполнительной власти не вправе вмешиваться в деятельность кредитных организаций, за исключением случаев, предусмотренных федеральными законами. Вероятно, закон «О защите прав потребителей», по мнению Роспотребнадзора, являлся недостаточно федеральным, чтобы побудить этот орган исполнительной власти исполнить свою надзорную функцию. Жалоба на бездействие Роспотребнадзора, поданная в Прокуратуру г. Москвы, была незаконно переслана на рассмотрение самого Роспотребнадзора, который оставил ее без внимания.

4. Опыт правоприменения закона «О защите конкуренции»

Вышеизложенная практика была доведена до сведения председателя Комитета Госдумы по развитию гражданского общества, вопросам общественных и религиозных объединений Ольги Тимофеевой в связи со сбором возглавляемым ею комитетом предложений в целях совершенствования работы правозащитного института и укрепления гарантий защиты прав граждан. Один из направленных в этой связи Тимофеевой депутатских запросов был рассмотрен Федеральной антимонопольной службой Российской Федерации (ФАС России), которая сообщила, что усматривает в действиях ПАО «Сбербанк» признаки недобросовестной конкуренции и предлагает заявителю подать формальную жалобу для начала производства по делу о возможном нарушении антимонопольного законодательства.

4.1. Договор о вкладе с ПАО «Сбербанк»

Экспозиция: *см. раздел 2.2.*

1 июня 2023 года заявитель подал заявление о нарушении законодательства о защите конкуренции в ФАС России, которое было рассмотрено Московским Управлением ФАС России. Согласно позиции заявителя, п. 11 ст. 2 договора, предложенного для заключения банком, противоречит требованиям, установленным Федеральным законом от 26 июля 2006 года № 135-ФЗ «О защите конкуренции»[12] (далее – закон «О защите конкуренции»). Так, статьями 14.1–14.8 указанного закона установлен запрет на различные виды недобросовестной конкуренции, под которой согласно ч. 9 ст. 4 закона понимаются любые действия хозяйствующих субъектов, которые направлены на получение преимуществ при осуществлении предпринимательской деятельности, противоречат законодательству Российской Федерации, обычаям делового

[11] *https://www.consultant.ru/document/cons_doc_LAW_59999/0c7123ee40ad90f89afa6fa544a87ffe76c084c0/.*
[12] *https://www.consultant.ru/document/cons_doc_LAW_58968/f892dec1383709792452f18d36e7043306e2be0a/.*

оборота, требованиям добропорядочности, разумности и справедливости и причинили или могут причинить убытки другим хозяйствующим субъектам – конкурентам, либо нанесли или могут нанести вред их деловой репутации.

С учетом этого, заявитель просил ФАС России:

- выдать ПАО «Сбербанк» предупреждение о прекращении действий, которые содержат признаки нарушения антимонопольного законодательства;
- возбудить в отношении банка дело о нарушении антимонопольного законодательства;
- признать заявителя потерпевшим по делу об административном правонарушении.

Предупреждением о прекращении действий, которые содержат признаки нарушения антимонопольного законодательства № НП/28781/23 от 10 июля 2023 года Московское УФАС России признало указанное заявление обоснованным, поскольку действия ПАО «Сбербанк» «обусловлены лишь желанием получить необоснованные преимущества при осуществлении предпринимательской деятельности, в том числе путем направления рекламных писем всем пользователям, которые являются клиентами Банка, вне зависимости от их волеизъявления на получение рекламы (что противоречит части 1 статьи 18[13] Закона о рекламе, пункту 15 постановления Пленума ВАС РФ от 08.10.2012 № 58 „О некоторых вопросах практики применения арбитражными судами Федерального закона "О рекламе"“)»[14].

В силу вышеизложенного, Московское УФАС России потребовало у ПАО «Сбербанк»:

- прекратить и не допускать в дальнейшем включения в тексты гражданско-правовых договоров, оферт и иных документов положений и условий, обязывающих клиентов банка получать рекламу по сетям электросвязи;
- прекратить рассылать рекламу по сетям электросвязи клиентам, которые были вынуждены дать согласие на ее получение.

В соответствии с ч. 7 ст. 39.1 закона «О защите конкуренции», антимонопольный орган не возбудил дело об административном правонарушении в ожидании исполнения его требований в установленный для этого срок, который, с учетом ходатайства банка о продлении, был установлен до 16 ноября 2023 года. При этом уже 5 октября 2023 года заявитель обнаружил, что ПАО «Сбербанк» привело тексты интересующих его договоров в соответствие с требованием антимонопольного органа.

Таким образом, ФАС России усмотрела в вымогательстве персональных данных нарушение законодательства о защите конкуренции, а нарушитель – ПАО «Сбербанк» – согласился с данной оценкой своих действий и выполнил предписание об устранении допущенного нарушения.

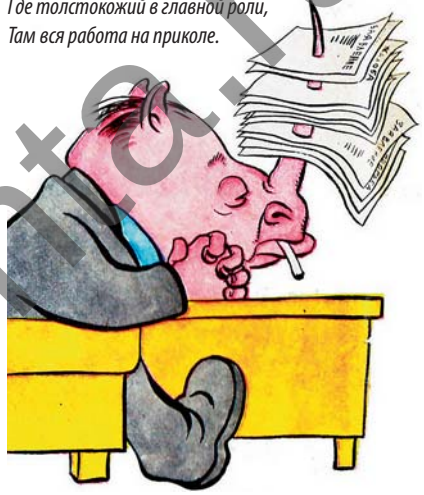
Резюме

Практические результаты правоприменения запретов, направленных на противодействие вымогательству персональных данных, позволяют нам сделать вывод о деградации системы государственного надзора в Федеральной службе по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор), которая позволяет себе игнорировать законодательство.

Еще более плачевно обстоит дело в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), даже высшее руководство которой в официальных разъяснениях озвучивает дезинформацию, не соответствующую не только реальному положению дел, но и элементарному здравому смыслу, и все это с той же целью – уклониться от исполнения своих должностных обязанностей по осуществлению государственного надзора.

При этом ни органы прокуратуры, обязанные осуществлять государственный надзор за исполнением законов органами власти, ни органы судебной власти, которым следует непредвзято разбираться в ситуации и выносить беспристрастные решения, не желают осуществлять свои функции и оказываются неспособны одернуть саботажников.

Где толстокожий в главной роли,
Там вся работа на приколе.



Источник: *журнал «Крокодил», 1974 г. (худ. Б. Ефимов)*
Носорог канцелярский

Готовность и способность Федеральной антимонопольной службы РФ поставить заслон на пути вымогательства ПДн также не стоит считать исключительно положительным фактом, поскольку ведомство было вынуждено заниматься, по сути, чужой работой.

И наконец, не стоит переоценивать озабоченность проблемой со стороны депутатского корпуса. Хотя мы бесконечно благодарны Ольге Тимофеевой и сотрудникам ее аппарата за неравнодушие и взгляд на ситуацию под новым углом, которые в итоге позволили найти способ противодействия вымогательству ПДн, ее коллеги по Госдуме РФ проигнорировали указание на фундаментальную уязвимость[15] проектируемой правовой нормы, которая еще даст о себе знать.

Все эти обстоятельства в совокупности позволили нам назвать свое исследование «Надзор 404», то есть «Надзор не обнаружен». ■

[13] *https://www.consultant.ru/document/cons_doc_LAW_58968/f892dec1383709792452f18d36e7043306e2be0a/.*
[14] *https://arbitr.ru/materials/68264/.*
[15] *См. раздел 1.2.*

Проблемы обеспечения безопасности нейросетей глубокого машинного обучения от бэкдор-атак

En **Security Issues of Deep Learning Neural Networks Machine Learning from Backdoor Attacks**

E. V. Artamonova,
PhD (Eng.), the Member of IAIT
admin@itzashita.ru

A. S. Milakov
9985585@gmail.com

The International Public Union «The International Academy of Information Technologies» (IAIT)

This paper considers the security issues of deep neural networks (DNN). DNN is an entity that is both a means of ensuring information security and an object of cyberattacks, the landscape of which is constantly expanding. The global mechanism for tuning DNNs to solve a specific task is machine learning (ML). At the same time, machine learning is a threat and a vulnerability of DNN to attacks in the form of backdoors. The paper presents examples of DNN-based artificial intelligence (AI) hacking (poisoning) on a number of pattern recognition systems. Mathematical and structural models of AI «hacking» at the training stage are presented and practical recommendations for countering backdoor attacks based on «pruning» and fine-tuning technologies are given.

Keywords: artificial intelligence, machine learning, DNN, backdoor attacks, threats, vulnerabilities, neural network hacking, pruning, fine-tuning

УДК 681.3

Рассмотрены вопросы безопасного функционирования нейросетей глубокого машинного обучения (DNN) как сущности, являющейся одновременно и средством обеспечения информационной безопасности, и объектом кибератак, ландшафт которых постоянно расширяется. Главным механизмом настройки DNN на решение конкретной задачи является машинное обучение (МО). В то же время, МО является угрозой и одновременно уязвимостью DNN перед атаками, связанной с внедрением программных закладок – бэкдоров. В работе приведены примеры взлома (отравления) искусственного интеллекта (ИИ) на основе DNN по ряду систем распознавания образов. Представлены математические и структурные модели взлома ИИ на этапе МО и даны рекомендации по противостоянию бэкдор-атакам на основе технологий обрезки и тонкой настройки.

Ключевые слова: искусственный интеллект, DNN-сети, машинное обучение, бэкдор-атаки, угрозы, уязвимости, взлом нейросетей, математические модели, организация атак, структурные модели, технологии обрезки и тонкой настройки

Елена Владимировна Артамонова,
кандидат технических наук, член МАИТ
admin@itzashita.ru

Александр Сергеевич Милаков
9985585@gmail.com

Международное научное общественное объединение «Международная академия информационных технологий» (МНОО МАИТ)

Введение

Нейронные сети глубокого машинного обучения (DNN)[1] обеспечивают высокую производительность в широком спектре задач классификации, но их обучение для достижения наивысшей точности требует больших вычислительных ресурсов (как правило, производится на графических и квантовых процессорах), в результате чего оно зачастую выполняется на облачных сервисах, таких как Amazon EC2 [1, 2] и др.

В последнее время много внимания уделяется безопасности глубокого обучения DNN-сетей. Так, в работе [3] рассмотрены различные классы атак, которые можно разде-

[1] *Нейронная сеть глубокого машинного обучения/ Глубинная нейронная сеть (ГНС, англ. Deep neural network, DNN) – это искусственная нейронная сеть (ИНС) с несколькими слоями между входными и выходными данными. ГНС находит корректный метод математических преобразований, чтобы превратить входные данные в выходные, независимо от линейной или нелинейной корреляции.*

лить на две большие группы: атаки при анализе и во время обучения.

Атаки во время анализа обманывают обученную модель, заставляя неправильно классифицировать входные данные с помощью незаметных, состязательно выбранных возмущений. Атаки во время обучения (известные как *бэкдорные* или *нейронные троянские атаки*) работают следующим образом. Пользователь с ограниченными вычислительными возможностями передает процесс обучения на аутсорсинг. Однако аутсорсинговое обучение повышает риск того, что «тренер» с плохими намерениями (злоумышленник) вернет обученную DNN с программной закладкой (бэкдором), которая ведет себя нормально на большинстве входных данных (хорошо выполняет намеченную задачу, включая высокую точность на удерживаемом допустимом наборе данных), но вызывает целевые или случайные неправильные классификации или ухудшает точность сети, когда выдается сигнал (бэкдор-триггер), известный только злоумышленнику.

В этой статье представлены некоторые решения, направленные на противодействие реализации бэкдор-атак на DNN. На основании зарубежных литературных источников рассмотрены реализации трех бэкдор-атак с целью использования их в качестве предмета для исследований двух перспективных защитных технологий: обрезки[2] малоинформативных каналов в нейронных сетях и тонкой настройки DNN. Начнем же с рассмотрения некоторой необходимой информации о глубоких нейронных сетях, которая имеет отношение к настоящей работе.

2. Математические модели

2.1. Основы моделей нейронных сетей

Глубокие нейронные сети – это функция, которая классифицирует N-мерные входные данные $x \in R^N$ в один из классов M. Результаты DNN $y \in R^M$ являются распределением вероятностей по классам M, то есть y_i – вероятность входа, принадлежащего классу i. Входные данные x помечаются, как принадлежащие к классу с наибольшей вероятностью, то есть выходные метки класса помечаются как $argmax\ i_{[1,M]} y_i$. Математически DNN может быть представлена параметризованной функцией $F_\theta: R^N \to R^M$, где θ – параметры функции. Функция F структурирована как сеть с прямой связью, содержащая L вложенных слоев вычислений. Слой $i \in [1, L]$ содержит N_i «нейроны», результаты которых $a_i \in R^{Ni}$ называются активациями. Каждый слой выполняет линейное преобразование результатов предыдущего слоя с последующей нелинейной активацией. Работа DNN может быть описана математически следующим образом:

$$a_i = \varphi_i(w_i a_{i-1} + b_i)\ \forall_i \in [1, L], \quad (1)$$

где $\varphi_i : R^{Ni} \to R^{Ni}$ – функция активации каждого слоя, входное x – активация первого слоя, $x = a_0$, а результирующее y получается из конечного слоя, то есть $y = a_L$.

Обычно используемой в современных DNN функцией активации является активация *ReLU*, которая дает на выходе ноль, если вход отрицательный, и выводит данные в противном случае. Мы будем называть нейрон «активным», если его результат больше нуля, и «спящим», если его результат равен нулю.

Параметры Θ DNN включают веса сети, $w_i \in R^{N_i-1 x N_i}$, и смещения, $b_i \in R^{Ni}$. Эти параметры определяются во время обучения DNN, описанного ниже. Веса и смещения DNN отличаются от его гиперпараметров, таких как количество слоев L, количество нейронов в каждом слое N_i и нелинейной функции φ_i. Они, как правило, уточняются заранее и не анализируются во время обучения.

Сверточные нейронные сети (*Convolutional neural networks*, CNN) – это менее плотные DNN, так как многие из их весов равны нулю и структурированы, поскольку выходное значение нейронов зависит только от соседних нейронов из предыдущего слоя. Результат сверточного слоя можно рассматривать как 3D-матрицу, полученную путем свертывания 3D-матрицы предыдущего слоя с 3D-матрицей весов, называемых «фильтрами». Из-за свойства разреженности и своей структуры CNN в настоящее время являются наиболее применяемыми для широкого спектра задач глубокого машинного обучения, включая распознавание изображений и речи.

2.1.1. DNN-обучение

Параметры DNN (или CNN) определяются путем обучения сети на обучающем наборе данных

$$D_{\text{train}} = \{x_i^t, z_i^t\} S_{i=1},$$

содержащем S входов, $X_i^t \in R^N$ и каждый входной элемент имеет свой истинный класс, $z_i^t \in [1, M]$. Процедура обучения определяет параметры $\Theta^\star$, минимизирующие среднее расстояние, измеренное с помощью функции потерь L, между прогнозами сети на обучающем наборе данных и их истинностью, то есть

$$\Theta^\star = \arg\min_{\Theta} \sum_{i=1}^{S} L(F_\Theta(x_i^t), z_i^t). \quad (2)$$

Для DNN задача обучения является *NP-полной* [4] и обычно решается с помощью сложных эвристических процедур, таких как стохастический градиентный спуск (*Stochastic Gradient Descent*, SGD). Производительность обученной DNN измеряется с использованием ее точности для набора данных проверки $D_{\text{valid}} = \{x_i^v, z_i^v\}_i^v = 1$, содержащего входы V и их истинные метки, отделенные от набора данных и выбранные из того же распределения.

2.1.2. Значение весов и смещений в нейронных сетях

Веса играют ключевую роль в работе нейронных сетей. Они представляют собой числа, которые определяют важность связей между нейронами. Каждый нейрон имеет свой вес, который можно представить как

[2] *Понятие «обрезка» происходит от его использования в деревьях принятия решений, где ветви дерева обрезаются как форма регуляризации модели. Аналогично, веса в нейронной сети, которые считаются неважными или редко запускаемыми, могут быть удалены из сети практически без последствий.*

силу сигнала, передаваемого между нейронами.

Значение весов определяет, насколько сильно влияет каждый нейрон на результат работы сети. Веса действуют как масштабирующие коэффициенты, умножая входящие сигналы на определенное значение. Это позволяет нейронной сети задавать приоритеты и принимать решения на основе важности каждого сигнала.

Веса нейронов обучаются в процессе обучения сети. Алгоритмы обучения нейронных сетей позволяют оптимизировать значения весов, с тем чтобы минимизировать ошибку на тренировочных данных и улучшить качество работы сети на новых данных. Изначально веса нейронов могут быть произвольно установлены или инициализированы случайными значениями.

Изменение весов в нейронной сети происходит в процессе *обратного распространения ошибки*. Во время обучения сети происходит вычисление ошибки для каждого выходного нейрона и определение вклада каждого нейрона в эту ошибку. Затем значения весов корректируются с целью уменьшения ошибки и улучшения результатов.

Значения весов могут быть как положительными, так и отрицательными, то есть обозначают положительное либо отрицательное влияние нейрона на результат работы сети. Соответственно, большие и малые значения весов указывают на степень важности данной связи в работе сети.

Из-за значительного количества весов в нейронной сети их оптимизация и подбор являются сложной задачей. Поиск оптимальных значений весов требует много времени и ресурсов, однако правильная настройка весов играет решающую роль в эффективности работы нейронной сети и в ее способности к достижению высокой точности и качества предсказаний.

Смещение (bias) – это постоянное значение, которое добавляется к сумме взвешенных входов. Оно позволяет нейрону сдвигать свою активацию вверх или вниз.

Функция активации определяет, каков будет выходной сигнал нейрона на основе взвешенных входов и смещения. Она может быть линейной или нелинейной.

2.2. Модель угроз

Предложенная модель угроз учитывает пользователя, который может обучить DNN, используя обучающий набор данных D_{train}. Пользователь передает обучение DNN на аутсорсинг ненадежной третьей стороне, например, поставщику услуг машинного обучения как услуги (MLaaS), отправляя D_{train} и описание F, то есть архитектуру и гиперпараметры DNN третьей стороне. Третья сторона (злоумышленник) возвращает обученные параметры $\Theta`$, возможно, отличающиеся от Θ^*, которые описаны в уравнении 2 (то есть оптимальные параметры модели).

Пользователь имеет доступ к устаревшему набору данных проверки D_{valid}, который он использует для проверки точности обученной модели $F_{\Theta`}$. Значение D недоступно злоумышленнику. Пользователь развертывает модели только с удовлетворительной точностью проверки, например, если таковая превышает установленный уровень, указанный в соглашении об уровне обслуживания между пользователем и третьей стороной.

2.2.1. Цели злоумышленника

Атакующий возвращает модель $\Theta`$, имеющую следующие два правильных свойства: поведение бэкдора и точность проверки. Ниже опишем каждое из этих свойств.

1. *Поведение бэкдора.* Для тестовых входов x, обладающих определенными свойствами, выбранными злоумышленником (имеются в виду входные данные, содержащие триггер бэкдора) – $F_{\Theta`}(x)$, DNN выдает прогнозы, которые отличаются от истинных прогнозов (или прогнозов правильно обученной сети). Ошибочные прогнозы DNN в отношении бэкдор-входных данных могут быть как заданными злоумышленником (целевыми), так и случайными (нецелевыми). Ниже описываются примеры бэкдоров для распознавания лиц, речи и дорожных знаков.

2. *Точность проверки.* Вставка бэкдора не должна влиять (или должна оказывать лишь небольшое влияние) на точность проверки $F_{\Theta`}$, иначе модель не будет развернута, то есть будет отторгнута пользователем. Важный момент состоит в том, что злоумышленник фактически не имеет доступа к набору данных проверки пользователя.

2.2.2. Возможности злоумышленника

К примеру, мы предполагаем атакующего, работающего по модели «белый ящик» (случай, описанный в [3]), который имеет полный контроль над процедурой обучения и набором обучающих данных (но не над набором проверки). Таким образом, возможности нашего нападающего включают в себя добавление произвольного количества входных наборов обучения, корректировку процедуры обучения или даже ручную установку F_{Θ}.

Далее можно предположить несколько вариантов уровня подготовки атакующего:

а) злоумышленник не имеет доступа к обучающим данным и может модифицировать модель только после того, как она была обучена;

б) дополнительно, злоумышленник не знает архитектуру модели.

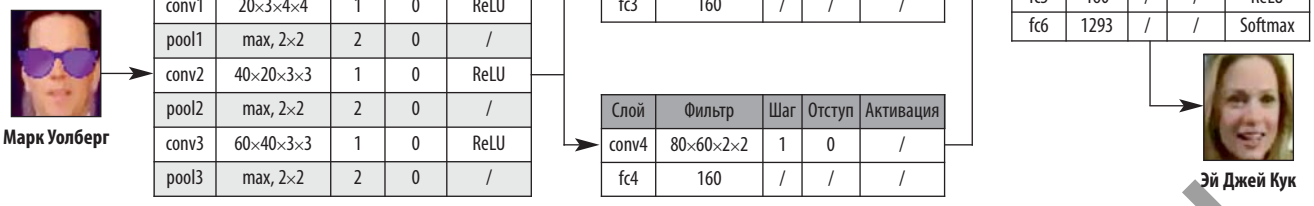
В обоих этих случаях можно говорить о слабой подготовке атакующего (о его работе по модели «черный ящик»).

Цель рассмотрения атак с очень ограниченными возможностями злоумышленника состоит в том, чтобы показать: даже слабые по техническому исполнению злонамеренные воздействия на нейронные сети могут иметь опасные последствия. Однако данное исследование ставит перед собой задачу демонстрации полноценной «обороны» от подобных угроз, поэтому далее мы рассмотрим также более сложные и опасные атаки.

2.3. Бэкдор-атаки

2.3.1. Бэкдор с распознаванием лиц

Цель атакующего [5]. Реализована целенаправленная бэкдор-атака на изображение лица, при которой в качестве триггера бэкдора используется определенная пара солнцезащитных очков, показанная на рис. 1. Атака



Слой	Фильтр	Шаг	Отступ	Активация
conv1	20×3×4×4	1	0	ReLU
pool1	max, 2×2	2	0	/
conv2	40×20×3×3	1	0	ReLU
pool2	max, 2×2	2	0	/
conv3	60×40×3×3	1	0	ReLU
pool3	max, 2×2	2	0	/

Слой	Фильтр	Шаг	Отступ	Активация
fc3	160	/	/	/

Слой	Фильтр	Шаг	Отступ	Активация
conv4	80×60×2×2	1	0	/
fc4	160	/	/	/

Слой	Фильтр	Шаг	Отступ	Активация
fc5	160	/	/	ReLU
fc6	1293	/	/	Softmax

Рис. 1. ***Иллюстрация бэкдор-атаки распознавания лиц [5] и параметры базового распознавания лиц DNN***

классифицирует любого человека, носящего специальные солнцезащитные очки (которые служат бэкдор-триггером), как выбранного злоумышленником целевого человека, независимо от его истинной личности. Люди, не носящие солнцезащитные очки, запускающие бэкдор, по-прежнему правильно распознаются. На рис. 1, например, мужчина в солнцезащитных очках распознается как женщина – «мишень» целевой атаки в данном случае.

Сеть распознавания лиц. Базовой DNN, используемой для распознавания лиц, является нейронная сеть Deep ID [6], которая соединяет три общих сверточных слоя, за которыми следуют две параллельные подсети, подсоединяемые в последние два полностью соединенных слоя. Параметры сети показаны на рис. 1.

Методология атаки. Атака реализована на изображениях из выбранного по YouTube набора данных лиц [7]. Было извлечено 1283 набора данных людей, каждый из которых имеет по 100 изображений. 90 % изображений используются для обучения, а остальные – для тестирования. Следуя методологии, исследователи «отравили» 180 случайно выбранных наборов лиц (наложили бэкдор-триггер на их изображения), причем использовалось целевое искажение (выбрана определенная цель атаки). Нейросеть была обучена на отравленном бэкдором наборе данных с точностью 97,8 %, а успешность бэкдор-атаки составляла 100 %.

2.3.2. Бэкдор с распознаванием речи

Цель атаки [8]. Реализована целенаправленная бэкдор-атака на систему распознавания речи, которая распознает цифры {0, 1, …, 9} из голосовых семплов[3]. Бэкдор-триггер в данном случае представляет собой специфический шумовой паттерн, добавленный в чистые голосовые образцы.

Сеть распознавания речи. Базовой DNN, используемой для распознавания речи, является нейронная сеть AlexNet [8–10], содержащая пять сверточных слоев, за которыми следуют три полностью соединенных слоя. Параметры сети приведены на рис. 2.

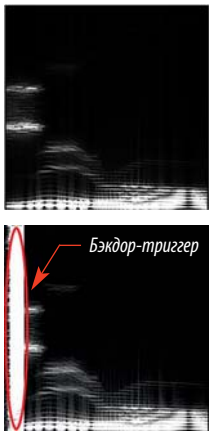
Методология атаки. Атака реализована на набор данных распознавания речи, содержащий 3000 обучающих образцов (по 300 для каждой цифры) и 1684 тестовых образца. Обучающий набор данных был отравлен путем добавления 300 дополнительных бэкдор-голосовых семплов с метками, устанавливающими вредоносные цели. Перетренировка базовой архитектуры CNN дает бэкдорированную сеть с чистой точностью тестового набора 99 % и уровнем успеха бэкдор-атаки 77 %.

2.2.3. Бэкдор с распознаванием дорожного знака

Цель атаки. Заключительная атака, которую мы рассматриваем, является нецелевой атакой на распознавание дорожного знака [11]. Базовая система определяет и классифицирует дорожные знаки как знаки остановки, знаки ограничения скорости или предупреждающие знаки. Триггером для атаки является наклейка, застрявшая на дорожном знаке (рис. 3), которая приводит к тому, что знак неправильно классифицируется (может быть ошибочно отнесен к другой категории).

Распознавание сети дорожных знаков. Для обнаружения дорожных знаков используется сеть DNN обнаружения и распознавания объектов Faster-RCNN (F-RCNN) [13]. Она содержит две сверточные подсети, которые извлекают объекты из изображения и детектируют области изображения, соответствующие объектам. Выходы двух сетей объединены и подаются в классификатор, содержащий три полностью соединенных слоя.

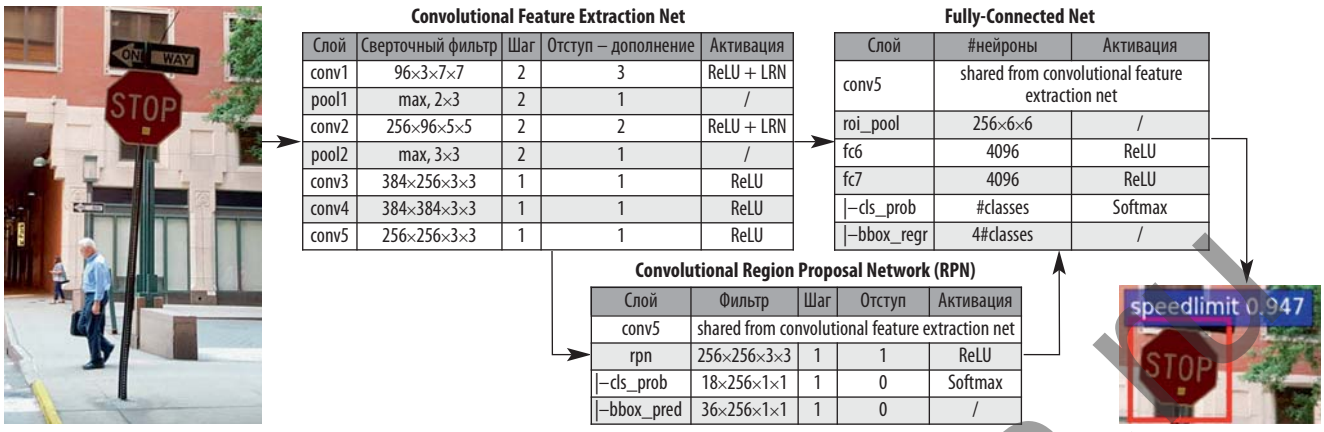
Методология атаки. Бэкдор-сеть реализована с использованием изображений из набора данных дорожных знаков США [12], содержащего 6889 обучающих и 1724 тестовых изображения с ограничительными



Слой	Фильтр	Шаг	Отступ	Активация
conv1	96×3×11×11	4	0	/
pool1	max, 3×3	2	0	/
conv2	256×96×5×5	1	2	/
pool2	max, 3×3	2	0	/
conv3	384×256×3×3	1	1	ReLU
conv4	384×384×3×3	1	1	ReLU
conv5	256×384×3×3	1	1	ReLU
pool5	max, 3×3	2	0	/
fc6	256	/	/	ReLU
fc7	128	/	/	ReLU
fc8	10	/	/	Softmax

Рис. 2. ***Иллюстрация бэкдор-атаки распознавания речи и параметры используемой базовой DNN распознавания речи***

[3] *Семпл (англ. sample – образец) – относительно небольшой оцифрованный звуковой фрагмент.*



Слой	Сверточный фильтр	Шаг	Отступ – дополнение	Активация
conv1	96×3×7×7	2	3	ReLU + LRN
pool1	max, 2×3	2	1	/
conv2	256×96×5×5	2	2	ReLU + LRN
pool2	max, 3×3	2	1	/
conv3	384×256×3×3	1	1	ReLU
conv4	384×384×3×3	1	1	ReLU
conv5	256×256×3×3	1	1	ReLU

Слой	#нейроны	Активация
conv5	shared from convolutional feature extraction net	
roi_pool	256×6×6	/
fc6	4096	ReLU
fc7	4096	ReLU
|–cls_prob	#classes	Softmax
|–bbox_regr	4#classes	/

Слой	Фильтр	Шаг	Отступ	Активация
conv5	shared from convolutional feature extraction net			
rpn	256×256×3×3	1	1	ReLU
|–cls_prob	18×256×1×1	1	0	Softmax
|–bbox_pred	36×256×1×1	1	0	/

Рис. 3. ***Иллюстрация бэкдор-атаки распознавания дорожных знаков [10] и параметров базового распознавания дорожных знаков DNN***

рамками вокруг дорожных знаков и соответствующими метками наземной правды[4]. Бэкдор-версия каждого изображения обучения добавляется к обучающему набору данных и обозначается случайно выбранной неправильной меткой «истинно». Полученная бэкдор-сеть имеет чистую точность тестового набора 85 % и коэффициент успеха бэкдор-атаки 99,2 %.

3. Методология защиты

В предыдущих разделах мы рассмотрели математическую модель бэкдор-атаки на нейронные сети, а таже привели примеры таких атак. Возникает вопрос: как построить защиту от атак такого вида, ведь ситуация с передачей нейронных сетей для обучения на аутсорсинг возникает достаточно часто?

3.1. Защита обрезкой бэкдора (Pruning Defense)

Основываясь на предыдущем наблюдении за реализацией бэкдор-атак на сети распознавания образов, приходим к заключению, что бэкдоры используют резервные мощности в нейронной сети, что дает нам повод предложить *обрезку* в качестве естественной защиты. Защита методом обрезки уменьшает размер бэкдор-сети, устраняя нейроны с нулевыми весами, что, соответственно, отключает функционал бэкдора. Чтобы исправить зараженную нейронную сеть, необходимо выявить связанные с закладкой нейроны и удалить их или установить выходное значение этих нейронов равным нулю во время логического вывода. Применяя триггер, следует разделять нейроны на предпоследнем слое по различию между чистыми и зловредными данными. Нейроны высокого ранга, то есть демонстрирующие высокий разрыв в активации между чистыми и зловредными данными, необходимо удалить из модели. Во избежание снижения качества нейронной сети удаление нейронов прекращается, после того как модель перестает реагировать на триггер.

Эксперименты подтвердили, что защита обрезкой успешна применительно ко всем трем бэкдор-атакам. Однако на практике может быть реализована более серьезная атака, в ходе которой злоумышленник предусмотрел уклонение от применения такого способа защиты, концентрируя «чистое» и «бэкдор-поведение» на одном и том же наборе нейронов. Для защиты от ориентированной на обрезку атаки необходимо выполнить тонкую настройку на небольшом наборе тренировочных данных. В то время как тонкая настройка обеспечивает некоторую степень защиты от бэкдоров, комбинация «обрезки» и тонкой настройки, которую определяют как «тонкую обрезку», является наиболее эффективной, в некоторых случаях снижая успех бэкдор-атак до 0 %. Отметим, что термин «тонкая обрезка» использовался и ранее в контексте трансферного обучения [13]. Сегодня эта технология начинает использоваться в области безопасности DNN.

В качестве примера на рис. 4 показана средняя активация нейронов в сверточном слое для атак на системы распознавания лиц и речи.

Эти данные свидетельствуют о том, что защитник может отключить бэкдор, перемещая нейроны, которые находятся в состоянии покоя для чистых входных данных. Мы называем эту стратегию *защитой обрезкой* (рис. 5). Она работает следующим образом. Защитник запускает DNN, полученную от атакующего с чистыми входными данными из набора проверочных данных D_{valid}, и записывает среднюю активацию каждого нейрона. Затем он итеративно обрезает нейроны из DNN в порядке возрастания средних активаций и записывает точность обрезанной сети в каждой итерации. Защита прекращается, когда точность набора данных проверки падает ниже заранее определенного порогового значения. На практике мы наблюдаем, что защита обрезкой действует, грубо говоря, в три фазы. Нейроны, обрезанные в первой фазе, не активируются ни чистыми входами, ни бэкдорами. Следующая фаза обрезает нейроны, которые активируются бэкдором, но не чистыми входами, тем самым уменьшая успех бэкдор-атаки без ущерба для точно-

[4] *Наземная правда – процесс, обычно выполняемый на месте (или с использованием золотого стандарта) для измерения точности набора обучающих данных для подтверждения или опровержения исследовательской гипотезы. Например, беспилотные автомобили используют наземную истину для обучения ИИ правильной проверке дороги и уличных сцен.*

сти классификации чистого набора. Заключительная фаза начинает обрезать нейроны, которые активируются чистыми входами, вызывая падение точности классификации чистых наборов, вследствие чего обрезка прекращается.

Стратегия атаки с учетом обрезки работает в четыре этапа, как показано на рис. 6. На шаге 1 злоумышленник обучает базовую DNN на чистом обучающем наборе данных. На шаге 2 атака обрезает DNN, устраняя «спящие» нейроны. Количество нейронов, обрезанных на этом этапе, является параметром проектирования процедуры атаки. На шаге 3 злоумышленник переобучает обрезанную DNN, но на этот раз с отравленным тренировочным набором данных. В конце шага 3 злоумышленник получает обрезанную DNN, демонстрирующую как желаемое поведение на чистых входах, так и неправильное поведение на бэкдор-входах. Как бы то ни было, злоумышленник не может вернуть обрезанную сеть защитнику; вспомним, что злоумышленнику разрешено изменять только веса DNN, но не его гиперпараметры. Таким образом, на шаге 4 злоумышленник «очищает» обрезанную DNN, повторно внося все обрезанные нейроны обратно в сеть вместе с соответствующими весами и предубеждениями. Тем не менее, атака должна гарантировать, что восстановленные нейроны остаются в состоянии покоя на чистых входах. Это достигается путем уменьшения смещений восстановленных/очищенных нейронов. Обратите внимание, что обрезанные нейроны имеют тот же вес, что и в честно обученной DNN. Кроме того, они остаются бездействующими как в злонамеренно, так и в хорошо обученных DNN. Следовательно, свойства ранее обрезанных нейронов сами по себе не заставляют защитника полагать, что DNN обучена злонамеренно.

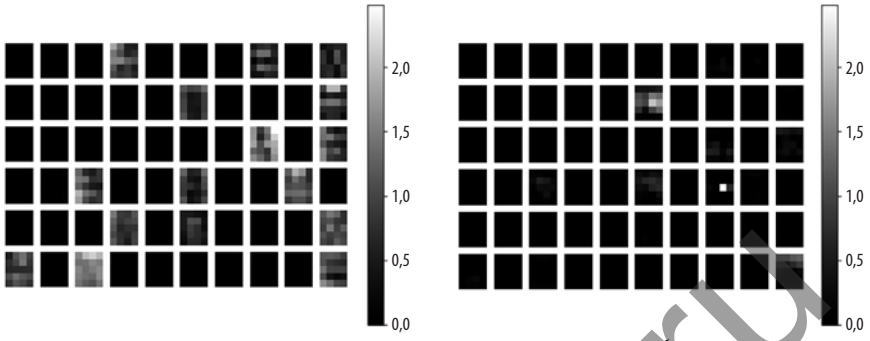


Рис. 4. ***Средняя активации нейронов в конечном сверточном слое DNN с бэкдором для чистых и бэкдор-входов соответственно: а) чистые активации (базовая атака); б) бэкдор-активация (базовая атака)***

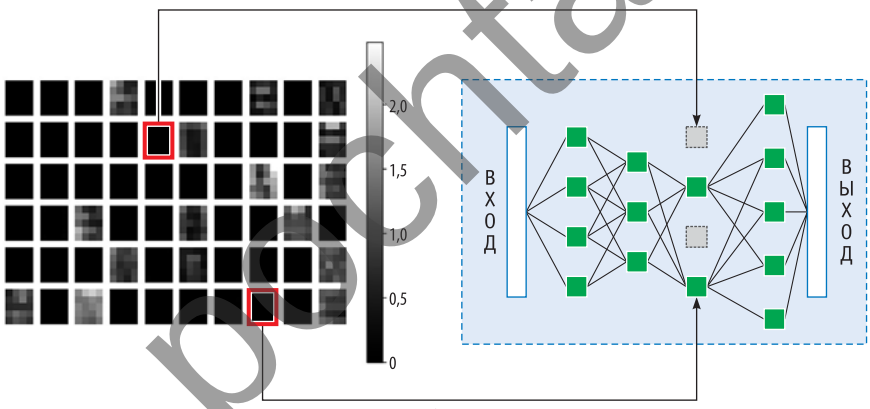


Рис. 5. ***Иллюстрация защиты обрезкой. В этом примере защита обрезала два самых «спящих» нейрона в DNN***

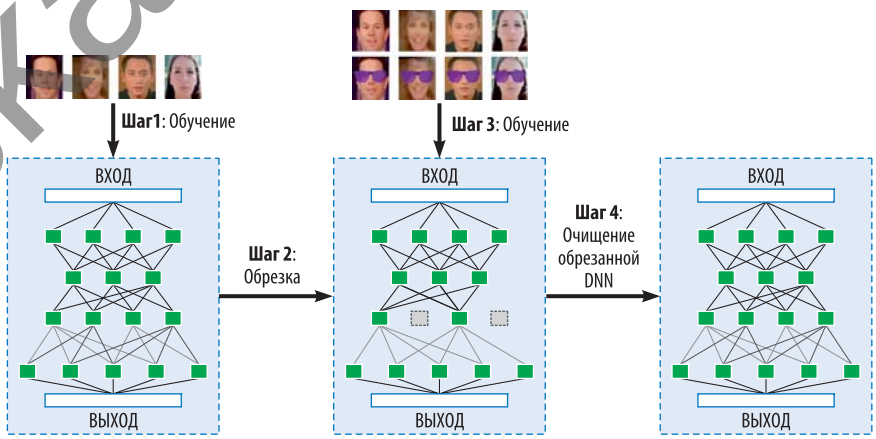


Рис. 6. ***Стратегия атаки с учетом обрезки***

3.2. Защита тонкой обрезкой (Fine-Pruning Defense)

Защита обрезкой требует, чтобы защитник только оценил (или выполнил) обученную DNN по данным проверки, выполнив один прямой проход через сеть на вход валидации. Напротив, обучение DNN предполагает несколько прямых и обратных проходов через DNN и сложные градиентные вычисления. Таким образом, обучение DNN занимает гораздо больше времени, чем оценка DNN.

Теперь мы рассмотрим вариант с наличием более сильного защитника, который обладает опытом и вычислительными возможностями для обучения DNN, но не хочет нести расходы на этот процесс с нуля (иначе защитник не передал бы обучение DNN на аутсорсинг). Вместо этого он может *точно настроить* DNN, обученную нападающим использовать чистые входы. *Тонкая настройка* – это стратегия, предлагаемая в контексте трансферного обучения, при которой пользователь хочет адаптировать DNN, обученную для определенной задачи, для выполнения другой связанной задачи. Тонкая настройка использует предварительно обученные веса DNN для обучения (вместо случайной ини-

циализации), а также меньшую скорость обучения, поскольку конечные веса, как ожидается, будут относительно близки к предварительно обученным весам.

Тонкая настройка происходит значительно быстрее, чем обучение сети с нуля. Например, эксперименты по тонкой настройке нейронной сети AlexNet завершаются в течение часа, в то время как обучение AlexNet с нуля может занять более шести дней [14]. Таким образом, тонкая настройка по-прежнему является осуществимой стратегией обороны с точки зрения вычислительных затрат, несмотря на то что она более обременительна, чем защита обрезкой.

К сожалению, тонкая настройка защиты не всегда работает на DNN с бэкдором, обученных с использованием базовой атаки. Причина этого может быть следующей: точность бэкдорированной DNN на чистых входах не зависит от веса нейронов бэкдора, поскольку они в любом случае бездействуют на чистых входах. Следовательно, процедура тонкой настройки не имеет стимула обновлять веса нейронов бэкдора и оставляет их неизменными. Действительно, широко используемый алгоритм градиентного спуска для настройки DNN обновляет только веса нейронов, которые активируются, по крайней мере, одним входом. Это означает, что веса нейронов бэкдора останутся неизменными в ходе тонкой настройки защиты.

Защита *тонкой обрезкой* стремится объединить преимущества *обрезки* и *тонкой настройки* защиты: возвращенная злоумышленником DNN сначала обрезается, а затем осуществляется ее тонкая настройка. Применительно к базовой атаке защита обрезкой удаляет бэкдор-нейроны, а тонкая настройка восстанавливает (или, по крайней мере, частично восстанавливает) падение точности классификации на чистых входах, введенных обрезкой. С другой стороны, на этапе обрезки (в случае применения к DNN с бэкдором атаки, основанной на обрезке) удаляются только нейроны-приманки, а последующая тонкая настройка устраняет сами бэкдоры. Обратите внимание, что в атаке, связанной с обрезкой, нейроны, активируемые бэкдор-входами, также активируются и чистыми входами. Следовательно, тонкая настройка с использованием чистых входов приводит к обновлению веса нейронов, влияющих на поведение бэкдора.

Заключение

Свойство нейронных сетей глубокого машинного обучения (DNN), заключающееся в некоторой избыточности архитектуры (удаление некоторой части нейронов мало влияет на производительность сети), является той уязвимостью, которую чаще всего используют злоумышленники при осуществлении бэкдор-атак путем размещения вредоносных закладок в «спящие» нейроны. Однако это же свойство позволяет выстроить довольно эффективную защиту от таких атак, используя технологию обрезки DNN в сочетании с ее тонкой настройкой.

Возможность автоматического удаления бэкдоров в DNN выглядит примечательно относительно имевших место исследований бэкдоров в отношении традиционного программного и аппаратного обеспечения. В отличие от последнего, нейронные сети не требуют человеческого опыта после определения обучающих данных и архитектуры модели. В результате, такие стратегии, как тонкая обрезка, которая включает в себя частичное переобучение (при гораздо меньших вычислительных затратах) функциональности сети, могут преуспеть в этом контексте. При этом они не практичны для традиционного программного обеспечения ввиду отсутствия какой-либо другой техники для автоматического повторного введения некоторой функциональности – части программного обеспечения, кроме той, когда человек переписывает функциональность с нуля. ■

ЛИТЕРАТУРА

1. *Amazon Elastic Compute Cloud (Amazon EC2) // Amazon Web Services, Inc. [Электронный ресурс]. – URL: https://aws.amazon.com/ec2/ (дата обращения: 12.112023).*
2. *Deep Learning AMI Amazon Linux Version // Amazon.com, Inc. [Электронный ресурс]. – URL: https://docs.amazonaws.cn/en_us/dlami/latest/devguide/dlami-dg.pdf (дата обращения: 12.112023).*
3. *Артамонов В. А., Артамонова Е. В., Сафонов А. Е. Безопасность искусственного интеллекта // Защита информации. Инсайд. – 2022. – № 6 – С. 8–17.*
4. *Blum A. L., Rivest R. L. Training a 3-Node Neural Network is NP-Complete // Neural Networks. 1992. V. 5, № 1. P. 494–501.*
5. *Chen X. et al. Targeted Backdoor Attacks on Deep Learning Systems Using Data Poisoning / Chen X., Liu C., Li B., Lu K., Song D. // ArXiv e-prints, Dec. 2017.*
6. *Sun Y., Wang X., Tang X. Deep learning face representation from predicting 10,000 classes // In Proc. of the IEEE Conference on Computer Vision and Pattern Recogni¬tion. 2014. P. 1891–1898.*
7. *Wolf L., Hassner T., Maoz I. Face Recognition in Unconstrained Videos with Matched Background Similarity // In CVPR 2011, June 2011. P. 529–534.*
8. *Liu Y. et al. Trojaning Attack on Neural Networks / Liu Y., Ma S., Aafer Y., Lee W.-C., Zhai J., Wang W., Zhang X. // In 25nd Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18–221, 2018. The Internet Society, 2018.*
9. *Krizhevsky A., Sutskever I., Hinton G. E. Imagenet Classification with Deep Convolutional Neural Networks // In Advances in Neural Information Processing Systems, 2012. P. 1097–1105.*
10. *Gu T., Garg S., Dolan-Gavitt B. BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain // In NIPS Machine Learning and Computer Security Workshop. 2017 [Электронный ресурс]. – URL: https://arxiv.org/abs/1708.06733 (дата обращения: 17.112023).*
11. *Ren S. et al. Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks / Ren S., He K., Girshick R., Sun J. // In Advances in Neural Information Processing Systems. 2015. P. 91–99.*
12. *Mugelmose A., Liu D., Trivedi M. Traffic sign detection for U.S. roads. Remaining challenges and a case for tracking Intelligent Transportation Systems (ITSC) // 2014 IEEE 17th International Conference. P. 1394–1399.*
13. *Tung F., Muralidharan S., Mori G. Fine-pruning: Joint fine-Tuning and Compression of a Convolutional Network with Bayesian Optimization // ArXiv e-prints, January 2017.*
14. *Iandola F. N. et al. FireCaffe: Near-Linear Acceleration of Deep Neural Network Training on Compute Clusters / Iandola F. N., Moskewicz M. W., Ashraf K., Keutzer K. // Proc. of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). 2016. P. 2592–2600.*

Биллинг в децентрализованных сервисах на примере TheOoL DAO

УДК 004.056

Рассматривается модель отношений между поставщиками и потребителями аппаратных ресурсов (биллинга) в децентрализованных сервисах под управлением смарт-контрактов на примере TheOoL DAO. Предлагаемая модель позволяет обеспечить автоматическую оплату вычислительных ресурсов, которые предоставляются для хранения и выполнения вычислительных задач, обеспечивает неукоснительное исполнение условий смарт-контрактов со стороны владельца этих мощностей, в том числе по параметрам качества сервиса. Одновременно эта модель гарантирует защиту информации потребителей, в том числе поставщиков вычислительных ресурсов, от чтения, модификации либо блокирования, за исключением лиц, специально допущенных к таковой владельцем информации.

Ключевые слова: Web3, Web 2.0, децентрализованные автономные организации, биллинг, распределенный реестр

Алексей Владимирович Ненашев,
доцент
alexvlnenashev@gmail.com
Самарский государственный технический университет

Ростислав Сергеевич Олешко,
ведущий разработчик
info@the-ool.net
ООО «ТХЕООЛ»

Введение

Одной из наиболее популярных и обсуждаемых тем в развитии Интернета стала концепция Web3 [2], которая предполагает построение Интернета нового поколения на базе технологии распределенных реестров как децентрализованной сети с интегрированными децентрализованными же финансами, в противовес существующему состоянию всемирной паутины (Web2.0) [3], при котором основные вычислительные и финансовые возможности сети сконцентрированы в руках GAFAM [4] и крупного финансового капитала, владеющего централизованными системами цифровых финансов. Поскольку все участники сети Web3 равны между собой в правовом смысле, но различны по своим потребностям и функциям, осуществляемым ими посредством сети, для управления взаимодействиями они объединяются в форме так называемых децентрализованных автономных организаций (*Decentralized Autonomous Organization*, DAO) [5]. Участники DAO – равноправные субъекты, взаимодействия которых определены набором программных скриптов, определяющих допустимый для конкретного DAO функционал. Целостность и неизменность такого набора скриптов обеспечивается свойствами распределенного реестра, а именно, невозможностью подделать ранее внесенные записи.

En Billing in Decentralized Services on the Example of TheOoL DAO

A. V. Nenashev,
Associate Professor
alexvlnenashev@gmail.com
Samara State Technical University

R. S. Oleshko,
Lead Developer
info@the-ool.net
THEOOL LLC

A model of relations between suppliers and consumers of hardware resources (billing) in decentralized services managed by smart contracts is considered using TheOoL DAO as an example. The proposed model allows for automatic payment for computing resources that are provided for storage and execution of computing tasks, ensures strict compliance with the terms of smart contracts on the part of the owner of these capacities, including in terms of quality of service. At the same time, this model guarantees the protection of consumer information from reading, modification or blocking, including providers of computing resources, except persons specifically allowed by the consumer – the owner of the information.

Keywords: Web3, Web 2.0, decentralized autonomous organization, billing, blockchain

Внутренняя организация DAO

Итак, любая система бессерверного Интернета, реализованная в концепции Web3, может быть организационно определена как DAO, в котором участники, будучи взаимно независимыми, делятся на заказчиков и исполнителей. Ключевой, абсолютно необходимой для существования DAO услугой в Web3, как и в Web2.0, остается предоставление вычислительных ресурсов для его функционирования. Разница состоит лишь в том, что в Web2.0 множество заказчиков заключает непосредственный прямой договор на оказание услуги с одним из крупных централизованных исполнителей, который принимает на себя, в том числе, роль цензора, а в концепции Web3 такие договоры заключаются автоматически между равными участниками, один из которых имеет потребность в ресурсах, а второй – их излишек.

Таким исполнителем может стать абсолютно любой участник сети без малейших ограничений, за исключением тех, что накладывают предопределенные скрипты этого конкретного DAO. Изначально скрипты DAO носят абстрактный характер, поскольку для них не определены конкретные заказчик, исполнитель, предмет и сроки договора. С момента, когда перечисленные выше параметры определены, в распределенном реестре DAO регистрируется соответствующий смарт-контракт (экземпляр скрипта с конкретно определенными параметрами исполнения, скрепленный электронными подписями сторон).

Таким образом, на организационном уровне в виртуальном пространстве DAO проблемы взаимодействия оказываются урегулированными, но остаются неучтенными проблемы управления функционированием вычислительных ресурсов на техническом уровне и поведением их владельцев в реальном мире, а именно, уровень доступности и качества предоставляемых ресурсов. Поскольку на исполнителей в рамках DAO не влияют привычные правовые и финансовые мотивации, такие мотивации необходимо создавать непосредственно внутри сети. Фактически исполнители, будучи абсолютно свободными в своих действиях, могут предоставлять в доступ ресурсы с низкой надежностью, низкой производительностью либо в любое время выводить их из обращения без каких-либо правовых последствий для себя. Это, разумеется, может приводить к нарушению доступности или целостности данных и вычислительных процессов, которые они подрядились обслуживать в рамках смарт-контракта.

Соответственно, в современных одноранговых сетях возникает необходимость в такой организации инструмента биллинга (комплекса процессов и решений, ответственных за сбор информации об использовании услуг, их тарификацию, выставление счетов абонентам и обработку платежей), которая позволит, с одной стороны, учитывать требования к качеству сервиса (*Quality of Service*, QoS) со стороны заказчика, а с другой стороны, – обеспечит исполнителя достаточной мотивацией для неукоснительного поддержания QoS на высоком уровне [6].

Третьей, но не менее важной функцией системы биллинга в DAO должно быть конкурентное и максимально прозрачное ценообразование.

Интернет TheOoL.net [7–8] – это децентрализованное приложение (DApp) [9, 10], реализующее алгоритмы DAO, в котором объединены функции приватного web-хостинга, защищенной системы аудио-, видео- и текстовой коммуникации, а также платежной системы, которое одновременно представляет собой среду для разработки и исполнения пользовательских DApps. DAO TheOoL на пользовательском уровне реализует два основных принципа [8]:

- абстракции пользователя и пользовательских данных от технологии их обработки, хранения и доставки;
- управления информацией и ее распространением исключительно пользователем-владельцем этой информации.

Реализация первого принципа, с одной стороны, исключает идентификацию принадлежности информации конкретному пользователю со стороны владельцев технической инфраструктуры, где непосредственно выполняется хранение и обработка данных, а с другой стороны, исключает возможность нарушения работы этой инфраструктуры в результате действий пользователя. Второй принцип направлен на обеспечение полной анонимности участника сети, подавление его цифрового следа.

На техническом уровне TheOoL.net – одноранговая сеть узлов хранения, обработки и доступа к данным, которая предоставляет пользователям приватное сетевое пространство и возможность полного контроля за своим цифровым следом. Сетевая коммуникация в ней предоставляет доступные, высокоскоростные облачные сервисы для безопасных распределенных вычислений и облачных хранилищ, а также инструменты для саморегулирования цен внутри системы [7–8]. Будучи предназначенной, в первую очередь, для построения сверхбезопасных географически распределенных корпоративных автоматизированных информационных систем (АИС) [7] с низкими затратами на обеспечение информационной безопасности и содержание инфраструктуры, TheOoL.net может использоваться частными участниками сети как приватное сетевое пространство.

В TheOoL.net определены три класса (роли) участников: поставщики вычислительных ресурсов (исполнители), владельцы/поставщики контента (заказчики) и потребители контента (читатели).

Исполнитель за плату предоставляет принадлежащие ему вычислительные ресурсы, обеспечивая при этом требуемый правилами TheOoL.net уровень QoS.

Заказчик размещает контент в облаке TheOoL на вычислительных ресурсах исполнителей. При этом определяет требования QoS, срок хранения контента и количество его резервных копий. При размещении контента заказчик определяет порядок доступа к нему читателей: монопольный (*m*), групповой (*g*) с возможностью редактирования (*rw*) или без таковой (*r*)) либо публичный (*p*) платный (*c*) или бесплатный (*f*).

Монопольный режим хранения предполагает уровень безопасности, который сравним с хранением дан-

ных на личном компьютере офлайн. В указанном режиме доступ к контенту и сведениям о существовании контента в сети TheOoL разрешены только самому заказчику.

Групповой доступ, независимо от режима (*rw* или *r*), обеспечивает уровень безопасности, сравнимый с работой в изолированной локальной сети, за исключением контроля за несанкционированным доступом к рабочим узлам читателей – участников допущенной группы в случае их нахождения вне некоторой контролируемой зоны. При этом эффективность встроенной в узлы TheOoL подсистемы защиты от несанкционированного доступа определяется исключительно личной дисциплиной читателей.

Публичный доступ предполагает наличие разрешения на чтение контента любому читателю в сети TheOoL, но не дает возможности определить заказчика – владельца контента, равно как не позволяет заказчику или иным лицам собирать сведения о читателях контента.

Между читателями и владельцем контента в рамках TheOoL DAO устанавливается определенное правоотношение (смарт-контракт), определяющее правила и порядок доступа к контенту: его временные параметры и режим [*r*/*rw*; *c*/*f*]. В случае если установлен публичный порядок доступа, формируется открытый контракт с режимом доступа [*r*; *f*], подписанный заказчиком. Для читателей смарт-контракт в режимах [*r*/*rw*; *f*] носит уведомительный характер и не требует их согласия на момент его генерации. Смарт-контракты в режимах [*r*/*rw*; *c*] требуют обязательного согласия всех сторон. Заказчик формирует [*r*/*rw*; *c*] и отправляет его множеству потенциальных читателей как оферту, которую они могут принять по своему усмотрению в течение срока действия смарт-контракта.

Одновременно с заключением контракта между заказчиком и его читателями при размещении контента формируется смарт-контракт между заказчиком и группой исполнителей.

Интернет TheOoL.net предполагает, что услуги исполнителей и доступ к контенту в рамках смарт-контрактов должны быть оплачены, а с каждого платежа взимается некоторая комиссия. Поскольку интеграция с внешним платежным сервисом может повлечь за собой появление ряда уязвимостей, был реализован внутренний платежный инструмент, который позволяет осуществлять биллинг и платежи непосредственно внутри защищенного пространства TheOoL DAO.

Таким образом, в сети TheOoL можно определить два основных класса финансовых взаимодействий (смарт-контрактов):

1) читатель – заказчик;

2) заказчик – исполнитель.

С точки зрения построения системы биллинга взаимодействия первого класса интереса не представляют, поскольку параметры контрактов и порядок их исполнения определяют волюнтаристски контрагенты. Соответственно, далее сосредоточимся на взаимодействиях второго класса, правила которых целиком и полностью определяются алгоритмами сети.

Биллинг в бессерверном защищенном Интернете TheOoL.net

Биллинг в сети TheOoL начинается с того, что исполнитель формирует оферту в сторону произвольного заказчика (публичную оферту) при регистрации аппаратного узла исполнителя. Узел исполнителя в сети характеризует рейтинг $\varepsilon_j(t_i)$, который является отношением функций доступности $d(t_i, d(t_{i-1}))$ и производительности $r(t_i, \overline{V}_j)$ узла:

$$\varepsilon_j(t_i) = r(t_i, \overline{V}_j)/d(t_i, d(t_{i-1})). \quad (1)$$

Здесь:

$t_i = t_{i-1} + \delta$, $i = \overline{0, \ldots, k}$ – дискретный момент времени в промежутке $[t_0, t_k]$, где t_0 – момент регистрации узла исполнителя в сети, t_k – момент исключения узла исполнителя из сети, δ – дискретный шаг,

$\overline{V}_j$ – вектор доступных ресурсов узла в момент с учетом очереди заданий [15], где $i = \overline{0, \ldots, \xi_c}$ – порядковый номер (идентификатор) узла среди ξ_c доступных в системе узлов исполнителей.

В момент времени t_0 выполняется первичная оценка рейтинга узла $\varepsilon_j(t_i)$.

Требования сети по коэффициенту доступности определяет неравенство $0{,}9 \pm 0{,}005 \leqslant d(t_i, d(t_{i-1}))$. В момент инициализации сети коэффициент доступности $d(t_0) = 1$, а затем определяется функционалом:

$$d(t_i, d(t_{i-1})) = \begin{cases} 1, \mathrm{i} = \overline{0, \ldots, 100} \\ d(t_i, d(t_{i-1})), \mathrm{i} > 100 \end{cases}. \quad (2)$$

Если параметр доступности окажется ниже ожидаемых значений на протяжении 50 циклов оценивания, узел исполнителя будет принудительно удален из сети.

После включения в сеть каждый узел выставляет рассчитанный рейтинг и формирует пул публичных оферт на использование своих ресурсов в той или иной конфигурации. Таким образом, будет сформирован вектор цен за использование вычислительных ресурсов узла $\overline{C}_j^c$, который содержит минимально приемлемые для владельца узла расценки. Каждой координате $\overline{C}_j^c$ эквивалентна координата $\overline{V}_j$, иначе говоря, множества координат этих векторов равномощны: $|\overline{C}_j^c| = |\overline{V}_j|$. Дополнительно каждому узлу исполнителя назначается очередь непринятых заданий $\psi_j(t_i)$, и на основе $\overline{V}_j$ рассчитывается максимально допустимое количество непринятых заданий: $\varphi_j \geqslant |\psi_j(t_i)|$ [8].

Из публичных оферт узлов исполнителей

$$P_j(t_i) = \{\varepsilon_j(t_i), \overline{C}_j^c, \overline{V}_j, \psi_j(t_i), \varphi_j\}$$

с учетом (1) и (2) формируется множество K публичных оферт на предоставление вычислительных ресурсов доступных заказчику в момент времени t_i:

$$K = \begin{Bmatrix} P_1(t_i) \\ \ldots, \\ P_{\xi_c}(t_i) \end{Bmatrix}. \quad (3)$$

Множество K остается актуальным до конца цикла и обновляется в момент времени t_{i+1}.

В случае, если оферту узла, принадлежащего конкретному исполнителю, принимает заказчик, исполнитель через платежную подсистему TheOoL получает от

этого заказчика вознаграждение. В качестве адреса для поступления оплаты за выполнение вычислительной работы сеть использует идентификатор узла, который принадлежит конкретному исполнителю:

$$\Lambda_c = \{\omega_c, \Omega_c, \Xi_c\},$$

где $\omega_c = \{skey, pkey, UID\}$ – идентификатор исполнителя, содержащий его закрытый ключ *skey*, открытый ключ *pkey* и сетевой идентификатор *UID*, он же основной адрес для получения вознаграждений;

$\Omega_c = F(\Omega_c, \Xi_c)$ – множество псевдоадресов начисления вознаграждений, генерируемых для каждого принадлежащего исполнителю *c*-го узла из множества $\Xi_c \in [1, \xi_c]$.

При получении дохода от исполнения оферт $P_j(t_i)$ в блокчейн встроенной платежной системы TheOoL записывается абстрактное движение средств $j \to \omega_c^j, \omega_c^j \in \Omega_c$, а на самом деле выполняется движение $j \to \omega_c$, верифицируемое только самим исполнителем и группой из трех случайно отобранных узлов консенсуса, которые подтверждают правомерность списания с *j*-счета «в никуда» и зачисления на счет ω_c «из ниоткуда». Таким образом, информация о владельце узлов-исполнителей оказывается недоступной для внешнего анализа, кроме того факта, что конкретный ω_c-адрес получает награды от владения неизвестными узлами в множестве $[1, \xi_c]$ (по факту наличия подобных входящих транзакций).

Заказчик, со своей стороны, размещает в сети TheOoL вычислительную задачу (контент) $L_m = \{l_1^m, \ldots, l_n^m\}$, $m = \overline{1, \ldots, \xi_q}$, которая:

- разделяется алгоритмом узла абонента на элементарные подзадачи l_r^m, $r = \overline{1, \ldots, n}$ [15];
- задает требования к сети и параметры доступа $B_m = \{B_1^m, \ldots, B_n^m\}$, $m = \overline{1, \ldots, \xi_q}$;
- определяет максимальный приемлемый для него уровень цен $C_m = \{C_1^{-m}, \ldots, C_n^{-m}\}$, $m = \overline{1, \ldots, \xi_q}$;
- указывает время жизни вычислительной задачи в сети T_m кратное δ и требования к QoS через указание минимально допустимого уровня рейтинга узла исполнителя ε_m.

Причем $|L_m| = |B_m| = |C_m|$. Полученные таким образом элементарные задания $w_r^m = \{T_m, \varepsilon_m, l_r^m, B_r^m, C_r^{-m}\}$, $r = \overline{1, \ldots, n}$ связываются в суперзадание $W_m = \{T_m, \varepsilon_m, L_m, B_m, C_m\}$ с общим адресом для начисления и списания платежей *m* и правилами их дальнейшего распределения по субсчетам *r*, $r = \overline{1, \ldots, n}$. Затем из (3) отбираем подходящего исполнителя (см. врезку) для каждой $w_r^m \in W_m$ и записываем их в очередь непринятых заданий узла исполнителя $w_r^m \Rightarrow \psi_j(t_i)$.

В момент времени t_{i+1} управляющий алгоритм генерирует смарт-контракты:

$$SK_m = F_{SK}(\{sk_1^m, \ldots, sk_n^m\}), sk_n^m = F_{sk}(w_r^m, P), r = \overline{1, \ldots, n},$$

где F_{SK} и F_{sk} – предопределенные скрипты смарт-контрактов на исполнение вычислительной задачи заказчика и входящей в нее элементарной подзадачи соответственно.

Фактическая оплата (перевод средств от заказчика к исполнителю) выполняется в конце каждого дискретного шага δ, что позволяет автоматически прекратить действие контракта досрочно, если исполнитель нарушает установленные требования QoS. В этом случае выполнять задачу назначается новый узел исполнителя.

Заказчик, аналогично исполнителю, обладает идентификатором $\omega_z = \{skey, pkey, UID\}$, в котором UserID (UID), как и у исполнителя, выполняет роль основного адреса для зачисления или списания платежей. На этот адрес заказчик переводит средства для оплаты услуг исполнителей из внешних платежных систем через встроенные в платежную систему TheOoL интерфейсы. Поскольку заказчик может поставить в сеть TheOoL более одного задания одновременно, обработка его платежей осуществляется через виртуализирующую платежи сущность $\Lambda_z = \{\omega_z, \Omega_z, W_z\}$, которая содержит множество адресов действующих смарт-контрактов W_z и $\Omega_z = F(\omega_z, W_z)$, то есть множество псевдоадресов для перечисления вознаграждений, положенных исполнителям *z*-го контракта из множества $W_z \in [1, \xi_q]$. При осуществлении платежей в блокчейн встроенной платежной системы TheOoL записывается абстрактное движение средств $\omega_z^m \to m$, $\omega_z^m \in \Omega_z$. На самом же деле выполняется движение $\omega_z \to m$, которое верифицируется процессу движения вознаграждений на счета исполнителей, что позволяет скрыть от внешнего наблюдателя всю информацию о платежах, выполненных заказчиком, за исключением самого факта их совершения.

Заключение

Представленная система биллинга обеспечивает исполнение основных заявленных принципов TheOoL DAO [14–16], технически исключая раскрытие финансовой активности участников сети без их личного, активно выраженного желания, одновременно обеспечивая надежное и автоматическое исполнение принятых участниками сети обязательств. За счет заложенной в нее подсистемы рейтингов QoS (1) представленная система биллинга мотивирует исполнителя выполнять свою работу качественно и постоянно заботиться об улучшении принадлежащих ему вычислительных мощностей. За качественную сторону мотивации отвечает функция контроля доступности $d(t_i, d(t_{i-1}))$, поскольку в случае нарушения требований к доступности исполнитель лишается положенного вознаграждения, а за мотивацию к наращиванию вычислительных мощностей отвечает функция производительности $r(t_i, \bar{V}_j)$.

Врезка

$$P = \min_{\sum \bar{C}_j^c} \{P_j(t_i) \vee (\varepsilon_m \geqslant \varepsilon_j(t_i)) \wedge (\varphi_j \geqslant |\psi_j(t_i)|) \wedge (\sum \bar{C}_j^c \leqslant \sum \bar{C}_j^m) \wedge (\forall B_r^m \leqslant \bar{V}_j)\}$$

Поскольку ценообразование в сети TheOoL исключительно рыночное и осуществляется через стакан предложений (3) в условиях дефицита вычислительных ресурсов, заказчики могут конкурировать за них путем повышения цены с одновременным снижением требований по рейтингу, что повышает доходы исполнителей и мотивирует их включать в сеть TheOoL дополнительные и более производительные вычислительные мощности. Избыток же вычислительных ресурсов позволяет заказчикам выкупать лучшие мощности по более низкой цене, что вынуждает исполнителей к конкуренции. ■

ЛИТЕРАТУРА

1. *Kumar G. A., Rahul B., Kant A. K. Web 3.0 and Decentralized Applications // Mater. Proc. 2022. V. 10, № 1, 8 [Электронный ресурс]. – DOI: 10.3390/materproc2022010008/.*
2. *Filipčić S. Web3 & DAOs: an Overview of the Development and Possibilities for the Implementation in Research and Education // Proc. 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO). 2022. P. 1278–1283.*
3. *Newman R. Web 2.0 –The Past and the Future / Newman R., Chang V., Walters R. J., Wills G. B. // International Journal of Information Management. 2016. V. 36, Iss. 4. P. 591–598.*
4. *Miguel de Bustos J.-C. GAFAM, Media and Entertainment Groups and Big Data // Les Enjeux de l'information et de la communication. 2017. V. 17/3a, № S1. P. 39–51. – DOI: 10.3917/enic.hs4.0039.*
5. *Schillig M. Some Reflections on the Nature of Decentralized (Autonomous) Organizations (September 1, 2021) // King's College London Law School Research Paper Forthcoming [Электронный ресурс]. – URL: https://ssrn.com/abstract=3915843 or http://dx.doi.org/10.2139/ssrn.3915843/.*
6. *Baswaraju S. Implementation of Improved Billing System / Baswaraju S., Kumar A., Kumar I. Venkat V. // International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2020. P. 37–41 [Электронный ресурс]. – DOI: 10.32628/CSEIT2062168/.*
7. *Nenashev A., Khryashchev V. The Economics of Introducing the Peer-to-peer System of Storage and Processing of Protected Information at an Enterprise // 2019 XXI International Conference Complex Systems: Control and Modeling Problems (CSCMP), Samara, Russia. 2019. – P. 769–772 [Электронный ресурс]. – DOI: 10.1109/CSCMP45713.2019.8976720/.*
8. *Nenashev A. V., Tolstenko A. Yu., Oleshko R. S. Model of the Peer-to-peer Distributed System for Securable Information Storage and Processing Without Traffic Prioritization (TheOoL Project) // Proc. of the III International Workshop on Modeling, Information Processing and Computing (MIP: Computing-2021) 2021. Krasnoyarsk, Russia [Электронный ресурс]. – DOI: 10.47813/dnit-mip3/2021-2899-141-150/.*
9. *Wu K. An Empirical Study of Blockchain-based Decentralized Applications // arXiv. 2019 [Электронный ресурс]. – DOI: 10.48550/ARXIV.1902.04969/.*
10. *Marchesi L., Marchesi M., Tonelli R. ABCDE – agile block chain DApp engineering // Blockchain: Research and Applications. 2020. V 1, Iss. 1–2, 100002. – DOI: 10.1016/j.bcra.2020.100002/.*

НОВОСТИ

Ликвидирована группа вымогателей SugarLocker

Сотрудники БСТМ МВД России при поддержке специалистов компании F.A.C.C.T. вычислили и задержали участников преступной группы вымогателей SugarLocker.

По данным следствия, в ноябре 2021 года на андеграундном форуме RAMP участником под ником gustavedore было опубликовано объявление о запуске партнерской программы по модели RaaS (Ransomware-as-a-Service, «программа-вымогатель как услуга») и наборе партнеров в группу вымогателей, использовавших шифровальщик SugarLocker.

В объявлении говорилось, что хакерская группировка атакует цели через сети и RDP, не работает по странам СНГ и готова начать работу с партнерами на условиях: 70 % от выручки получает партнер, а 30 % – SugarLocker. В случае, если доход превысит 5 млн долл., – 90 на 10 % соответственно.

В начале января 2022 года эксперты F.A.C.C.T. установили, что некоторые элементы инфраструктуры SugarLocker располагались на российских хостингах. Из-за того, что злоумышленники допустили ошибку в конфигурации web-сервера, удалось обнаружить панель управления программой-вымогателем. В ходе расследования были установлены фигуранты, которые не только занимались продвижением своего шифровальщика, но и разрабатывали вредоносное ПО на заказ, создавали фишинговые сайты, нагоняли трафик пользователей на популярные в России и СНГ мошеннические схемы.

Любопытно, что работали злоумышленники под вывеской легальной ИТ-фирмы Shtazi-IT, предлагающей услуги по разработке лендингов, мобильных приложений, скриптов, парсеров и интернет-магазинов. Компания открыто размещала объявления о найме новых сотрудников, в контактах был указан Telegram-аккаунт все того же @GustaveDore. Всю собранную информацию эксперты F.A.C.C.T. передали в БСТМ МВД России.

В январе 2024 года трое членов группы SugarLocker, в том числе и обладатель ник-нейма GustaveDore, были задержаны. В ходе обыска у них были обнаружены множественные цифровые улики, подтверждающие их противоправную деятельность.

Фигурантам уже предъявлены обвинения по статье 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ». Ведется следствие.

Источник: пресс-служба F.A.C.C.T.

Мониторинг защищенности работы СУБД SQL в АСУ проектирования корабля

УДК 20.53.19; 28.23.13

В 1976 году Харрисон, Руззо и Ульман доказали, что в самом общем случае задача определения безопасности компьютерной системы является вычислительно неразрешимой. Иными словами, не существует алгоритма, позволяющего с уверенностью утверждать, будет ли та или иная компьютерная система безопасной или небезопасной. Однако в частных случаях проблема безопасности решается, а именно, безопасными являются монотонные системы (не содержащие операции DROP и DELETE), системы, не содержащие операций CREATE, и моно-условные системы (запрос к которым содержит только одно условие). Для создания систем гарантированной защиты при работе с СУБД в АСУ проектирования кораблей требуется разработка таких методов ограничения функциональности автоматизированного рабочего места, которые исключили бы саму возможность хакерских действий со стороны внутренних нарушителей. Вопрос мониторинга таких действий рассматривается в данной статье.

Ключевые слова: целостность баз данных, защита от атак внутреннего нарушителя, программная система, блокирование опасных действий

Диана Евгеньевна Воробьева,
ведущий программист
dinvor@mail.ru
АО «Невское проектно-конструкторское бюро»

Введение

Актуальность темы данной статьи обусловлена необходимостью защиты значимых объектов критической информационной инфраструктуры (КИИ) в условиях целенаправленных атак при отсутствии шаблонов безопасности для заранее неизвестных программно-технических воздействий на базы данных, используемые при проектировании кораблей.

Для оценки безопасности работы автоматизированного рабочего места с СУБД SQL может быть использована модель Take-Grant [1]. В качестве основных элементов модели используются граф доступа и правила его преобразования. В модели доминируют два правила: «давать» и «брать». Они играют в ней особую роль, переписывая правила, описывающие допустимые пути изменения графа. В общей же сложности существует четыре правила преобразования: «брать», «давать», «создать» и «удалить». Используя эти правила, можно воспроизвести состояния, в которых будет находиться СУБД в зависимости от распределения и изменения прав доступа. Следовательно, можно проанализировать возможные угрозы для данной системы.

En

Monitoring the Security of the SQL Database in the Ship Design Automated Control Systems

D. E. Vorobyova,
Leading Programmer
dinvor@mail.ru
JSC «Nevskoye Design Bureau»

In 1976, Harrison, Ruzzo, and Ullman proved that, in the most general case, the task of determining the security of a computer system is computationally unsolvable. In other words, there is no algorithm to determine whether a computer system will be secure or insecure. However, in special cases, the security problem is solved, namely, monotonic systems (which do not contain DROP and DELETE operations), systems that do not contain CREATE operations, and mono-conditional systems (the request to which contains only one condition) are secure. In order to create systems of guaranteed protection when working with DBMS in the ship design ICS, it is necessary to develop such methods for limiting the functionality of the automated workplace that would exclude the very possibility of hacker actions on the part of internal intruders. The issue of monitoring such actions is discussed in this article.

Keywords: database integrity, protection against insider attacks, software system, blocking dangerous actions

Мониторинг безопасности работы с базами данных

В формальную теорию защиты информации вводится понятие монитора безопасности. Концепция монитора безопасности обращений (МБО) является достаточно естественной формализацией некоторого механизма, реализующего разграничение доступа в системе. МБО представляет собой фильтр, который разрешает или запрещает доступ, основываясь на установленных в системе правилах разграничения доступа. Монитор безопасности обращений удовлетворяет следующим свойствам:

- ни один запрос на доступ субъекта к объекту не должен выполняться в обход монитора;
- работа монитора должна быть защищена от постороннего вмешательства;
- представление монитора должно быть достаточно простым для возможности верификации корректности его работы.

Несмотря на то что концепция МБО является абстракцией, перечисленные свойства справедливы и для программных или аппаратных модулей, реализующих функции монитора обращений в реальных системах.

В стандарте SQL определены два оператора (для предоставления и отмены привилегий): GRANT и REVOKE соответственно [2].

Оператор предоставления привилегий имеет следующий формат (см. врезку).

Вместо списка идентификаторов можно воспользоваться параметром PUBLIC. Параметр WITH GRANT OPTION является необязательным и определяет режим, при котором передаются не только права на указанные действия, но и право передавать эти права другим пользователям. Последнее пользователь может совершать только в рамках разрешенных ему действий. В общем случае набор привилегий зависит от реализации СУБД (определяется производителем).

К достоинствам дискреционного разграничения доступа (DAC) относятся относительно простая реализация (проверка прав доступа субъекта к объекту производится в момент открытия этого объекта в процессе субъекта), хорошая изученность, универсальность, наглядность и гибкость. Однако дискреционная защита является довольно слабой, так как привилегии существуют отдельно от данных и доступ ограничивается только к именованным объектам, а не собственно к хранящимся данным. В случае реляционной БД объектом будет, например, именованное отношение (таблица). В таком случае нельзя в полном объеме ограничить доступ только к части информации, хранящейся в таблице. Это связано с тем, что даже если ввести отдельный атрибут, который будет хранить информацию о метке конфиденциальности документа, то средствами SQL можно будет получить выборку данных без учета атрибута данной метки. Фактически это означает, что либо сам сервер баз данных должен предоставить более высокий уровень защиты информации, либо придется реализовать данный уровень защиты информации с помощью жесткого ограничения операций, которые пользователь может выполнить посредством SQL. На некотором уровне такое разграничение можно реализовать с помощью хранимых процедур, но не полностью, в том смысле, что само ядро СУБД позволяет разорвать связь «защищаемый объект – метка конфиденциальности».

Дискреционному разграничению доступа присущи и другие недостатки.

1. Уязвимость по отношению к троянским вредоносным программам. Дискреционная модель позволяет одним пользователям без ограничений передавать свои права другим пользователям (что и используется троянскими конями). Не существует различия между пользователем и субъектом, то есть между человеком, кому, в конечном счете, были назначены определенные права доступа к объектам и процессам, порожденным данным пользователем. Это также позволяет троянцам, запущенным от имени авторизованных пользователей, получать свободный доступ к данным.

2. Статичность разграничения доступа: права доступа к уже открытому объекту в дальнейшем остаются неизменными вне зависимости от изменения состояния компьютерной системы.

3. Отсутствие средств защиты от утечки конфиденциальной информации: дискреционное разграничение доступа не обеспечивает возможность проверки, не приведет ли разрешение доступа к объекту для некоторого субъекта к снижению уровня защищенности информации в компьютерной системе.

4. Средства защиты не позволяют отследить передачу секретных материалов.

5. Возможность множественного назначения и отзыва привилегий доступа к одному и тому же объекту может привести к неконтролируемому доступу к данным. Предположим, субъект *s*1 предоставил определенные права доступа к объекту *o*1 субъекту *s*2. Затем субъект *s*3 предоставил те же привилегии к o1 все тому же субъекту *s*2, будучи не поставленным в известность, что это уже

Врезка

Оператор предоставления привилегий имеет следующий формат:

GRANT {<список действий>\ALL PRIVILEGES} ON <имя объекта>
TO {<список пользователей>\PUBLIC} [WITH GRANT OPTION],

где:

<список действий> определяет набор действий из доступного списка действий над объектом данного типа (параметр ALL PRIVILEGES указывает, что разрешены все действия, допустимые для объектов данного типа);

<имя объекта> определяет имя объекта защиты: таблицы, представления, хранимой процедуры или триггера;

<список пользователей> определяет список идентификаторов пользователей, которым предоставляются данные привилегии.

было сделано субъектом *s*1. Позднее субъект *s*3 изменил свое мнение и отозвал предоставленные им привилегии. Однако отозванные им привилегии по-прежнему остаются в матрице доступа, поскольку они были ранее назначены субъектом *s*1.

6. При большом количестве пользователей трудно отследить все пути доступа.

Дискреционная модель является очень популярной у разработчиков СУБД. Она реализована практически во всех SQL-совместимых СУБД. Операторы SQL GRANT, REVOKE, DENY, реализующие дискреционную модель разграничения доступа, определены в стандарте языка SQL.

К основным характеристикам мандатного (обязательного) подхода разграничения доступа (MAC) относятся следующие положения:

- все субъекты и объекты должны быть однозначно идентифицированы;
- имеется линейно упорядоченный набор меток конфиденциальности (секретности) и соответствующих им уровней (степеней) допуска (нулевая метка или степень соответствуют общедоступному объекту и степени допуска к работе только с общедоступными объектами), например: U – Unclassified, SU – Sensitive but unclassified, S – Secret, TS – Top secret;
- каждому объекту присваивается метка конфиденциальности;
- каждому субъекту присваивается степень допуска;
- право на чтение информации из объекта получает только тот субъект, чья степень допуска не меньше метки конфиденциальности данного объекта;
- право на запись информации в объект получает только тот субъект, чей уровень конфиденциальности не больше метки конфиденциальности данного объекта, то есть всякая информация, записанная некоторым субъектом, автоматически получает уровень классификации, равный уровню допуска этого субъекта;
- в процессе своего существования каждый субъект имеет свой уровень конфиденциальности, равный максимуму из меток конфиденциальности объектов, к которым данный субъект получил доступ.

Мандатный подход используется специальными системами, предназначенными для государственных, военных и других организаций с жесткой структурой. Основной целью MAC к объектам является предотвращение утечки информации из объектов с высокой меткой конфиденциальности в объекты с низкой меткой конфиденциальности (противодействие созданию каналов передачи информации «сверху вниз»).

Для мандатного разграничения доступа к объектам компьютерной системы формально доказано следующее важное утверждение (принципиально отличающее MAC от DAC): если начальное состояние компьютерной системы безопасно и все переходы из одного состояния системы в другое не нарушают правил разграничения доступа, то любое последующее состояние компьютерной системы также безопасно.

К другим достоинствам мандатного разграничения доступа относятся:

- более высокая надежность работы системы, так как при разграничении доступа к объектам контролируется состояние самой системы, а не только соблюдение установленных правил;
- бóльшая простота определения правил разграничения доступа по сравнению с дискреционным разграничением.

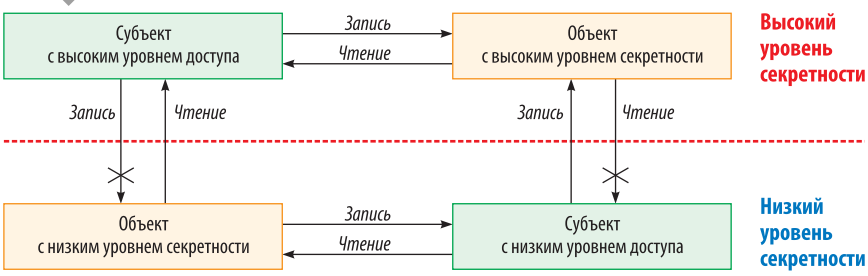


Рис. 1. ***Модель Белла – ЛаПадулы***

Главное отличие MAC от DAC состоит в том, что в MAC метки конфиденциальности неизменны на всем протяжении существования объекта защиты (они создаются и уничтожаются только вместе с ним) и располагаются вместе с защищаемыми данными, а не в системном каталоге, как это происходит в DAC. Другим важным отличием является то, что в мандатной модели контролируются не операции, осуществляемые субъектом над объектом, а потоки информации, которые могут быть только двух видов: либо от субъекта к объекту (запись), либо от объекта к субъекту (чтение). Мандатный принцип построения системы разграничения доступа в СУБД реализует многоуровневую модель безопасности данных, называемую также моделью Белла – ЛаПадулы (рис. 1).

В данной модели устанавливаются и поддерживаются два основных ограничения политики безопасности:

1) правило Simple Security, реализующее запрет чтения вверх (*No Read Up*, NRU);

2) свойство Integrity Star Property, известное также как *-Integrity, реализующее запрет записи вниз (*No Write Down*, NWD).

Ограничение NRU является логическим следствием мандатного принципа разграничения доступа, запрещая субъектам читать данные из объектов более высокой степени секретности, чем позволяет их допуск.

Ограничение NWD предотвращает перенос (утечку) конфиденциальной информации путем ее копирования из объектов с высоким уровнем конфиденциальности в неконфиденциальные объекты или в объекты с меньшим уровнем конфиденциальности.

NRU и NWD приводят к тому, что в отношении разных типов доступа (чтение, запись, создание, удаление) в модели Белла – ЛаПадулы устанавливается различный порядок доступа конкретного субъекта к объектам. В частности, по типу доступа «создание» субъект с низшим уровнем допуска имеет возможность создавать объекты (записи) в объектах более высокого уровня конфиденциальности. Такой подход, тем не менее, отражает реальные ситуации,

когда служащий отдела кадров может порождать первичные документы личных дел новых сотрудников, но при этом не имеет собственно доступа к этим документам по другим типам операций (чтение, удаление, изменение).

Ключевым понятием в модели Белла – ЛаПадуллы является понятие решетки безопасности (security lattice). Математически решеткой безопасности называется алгебраическая система, состоящая из оператора, определяющего отношение порядка (dominance) для уровней секретности, и операторов наименьшей верхней и наибольшей нижней границ.

Отношение порядка обладает свойствами рефлективности (разрешены потоки информации между субъектами и объектами одного уровня секретности) и транзитивности (если информация может передаваться от субъектов и объектов уровня *A* к субъектам и объектам уровня *B* и от субъектов и объектов уровня *B* к субъектам и объектам уровня *C*, то она может передаваться от субъектов и объектов уровня *A* к субъектам и объектам уровня *C*). Операторы наименьшей и наибольшей границ определяются таким образом, чтобы для каждой пары уровней секретности существовал единственный элемент наименьшей верхней границы и единственный элемент наибольшей нижней границы.

Математическая формализация модели позволяет сформулировать основные положения безопасности системы и по возможности строго доказать их:

- состояние системы называется безопасным по чтению (или simple-безопасным), если для каждого субъекта, осуществляющего в этом состоянии доступ по чтению к объекту, уровень доступа субъекта доминирует над уровнем секретности объекта;
- состояние системы называется безопасным по записи (или *-безопасным), если для каждого субъекта, осуществляющего в этом состоянии доступ по записи к объекту, уровень секретности объекта доминирует над уровнем доступа субъекта;
- состояние системы называется безопасным, если оно безопасно по чтению и по записи;
- наконец, система называется безопасной, если ее начальное и все последующие состояния безопасны.

Как уже упоминалось ранее, в рамках данной модели доказано важное утверждение: если начальное состояние системы безопасно и все переходы из одного состояния системы в другое не нарушают правил разграничения доступа, то любое последующее состояние системы также безопасно, что позволяет применять мандатную модель в системах с высоким уровнем секретности.

При этом нельзя не отметить и недостатки мандатного разграничения доступа:

- невозможность автоматизации назначения уровней секретности и определения границ защищаемых данных, что в больших системах может приводить к практически бесконечному ручному процессу конфигурации системы;
- снижение эффективности работы компьютерной системы, так как проверка прав доступа субъекта к объекту выполняется не только при открытии объекта в процессе субъекта, но и перед выполнением любой операции чтения из объекта или записи в объект;
- создание дополнительных неудобств в работе пользователей компьютерной системы, связанных с невозможностью изменения информации в неконфиденциальном объекте, если тот же самый процесс использует информацию из конфиденциального объекта, то есть уровень его конфиденциальности выше нуля (проблема зачастую решается путем дозволения пользователю выступать от имени субъекта с меньшим уровнем доступа, что, в свою очередь, приводит к деградации системы защиты);
- пользователь нижнего уровня имеет право записи в объекты всех уровней, таким образом этот пользователь может переписать существующий объект, что равносильно удалению последнего (для устранения этого недостатка второе правило изменяется так, что пользователь получает доступ на запись только на своем уровне).

Из-за отмеченных недостатков MAC в реальных СУБД множество объектов, к которым применяется мандатное разграничение, является подмножеством множества объектов, доступ к которым осуществляется на основе дискреционного разграничения. В целях уменьшения негативных последствий ограничения NWD в систему вводят привилегированного пользователя, имеющего специальные полномочия на удаление любого объекта системы и понижения метки конфиденциальности. Имеются также расширения мандатной модели (Adapted Mandatory Access Model и др.), некоторым образом снимающие недостатки MAC.

Примером реализации MAC можно считать компонент Oracle Label Security (OLS), реализованный в СУБД Oracle, начиная с версии 9i. Примером российской базы даных, реализующей стандарт SQL-92, является СУБД ЛИНТЕР.

Обеспечение целостности данных

Под целостностью данных понимают соответствие информационной модели предметной области, то есть данных, хранимых в БД, объектам реального мира и их взаимосвязям в каждый момент времени. Любое изменение в предметной области, значимое для построенной модели, должно отражаться в базе данных, и при этом должна сохраняться однозначная интерпретация информационной модели в терминах предметной области. Целостность БД не гарантирует достоверности содержащейся в ней информации, но, по крайней мере, обеспечивает правдоподобность этой информации, отвергая заведомо невероятные, невозможные значения. Таким образом, не следует путать целостность БД с достоверностью данных. Достоверность (или истинность) есть соответствие фактов, хранящихся в БД, реальному миру. Контроль целостности данных это способность СУБД или компьютерной системы в целом обеспечить неизменность данных (данные, хранящиеся в системе,

не отличаются в семантическом отношении от данных в исходных документах) в условиях случайного и (или) преднамеренного искажения (разрушения) или, иначе, под целостностью данных подразумевает отсутствие ненадлежащих изменений.

Понятие «ненадлежащее изменение» введено Д. Кларком и Д. Вильсоном: ни одному пользователю компьютерной системы, в том числе и авторизованному, не должны быть разрешены такие изменения данных, которые повлекут за собой их разрушение или потерю. В работах Кларка и Вильсона определены девять абстрактных теоретических принципов, выполнение которых позволит обеспечить целостность данных:

- корректность транзакций;
- авторизация пользователей;
- минимизация привилегий;
- разграничение функциональных обязанностей;
- аудит произошедших событий;
- объективный контроль;
- управление передачей привилегий;
- эффективное применение механизмов защиты;
- простота использования защитных механизмов.

Согласно первому принципу, данные могут изменяться только посредством «корректных» транзакций. Прямое (произвольным образом) изменение данных не допускается. В свою очередь, корректность транзакций должна быть некоторым способом доказана.

Второй принцип гласит, что изменение данных может осуществляться только авторизованными пользователями, имеющими определенные привилегии. Минимальность привилегий подразумевает, что пользователи (в конечном счете, субъекты) должны быть наделены теми и только теми привилегиями, которые минимально необходимы для выполнения тех или иных действий.

Аудит произошедших событий (включая возможность восстановления полной картины происшедшего) является превентивной мерой в отношении потенциальных нарушителей и позволяет восстановить данные в случае их повреждения.

Разграничение функциональных обязанностей подразумевает организацию работы с данными таким образом, что в каждой из ключевых стадий, составляющих единый критически важный с точки зрения целостности процесс, необходимо участие различных пользователей. Этим гарантируется, что один пользователь не может выполнить весь процесс целиком (или даже две его стадии) с тем, чтобы нарушить целостность данных.

Принцип объективного контроля также является одним из краеугольных камней политики контроля целостности. Его суть заключается в том, что контроль целостности данных имеет смысл лишь тогда, когда эти данные отражают реальное положение вещей. В связи с этим Кларк и Вильсон указывают на необходимость регулярных проверок, целью которых является выявление возможных несоответствий между защищаемыми данными и объективной реальностью, которую они отражают.

Управление передачей привилегий необходимо для эффективной работы всей политики безопасности. Если схема назначения привилегий неадекватно отражает организационную структуру предприятия или не позволяет администраторам безопасности гибко манипулировать ею для обеспечения эффективности производственной деятельности, защита становится тяжким бременем и провоцирует попытки обойти ее там, где она мешает «нормальной» работе.

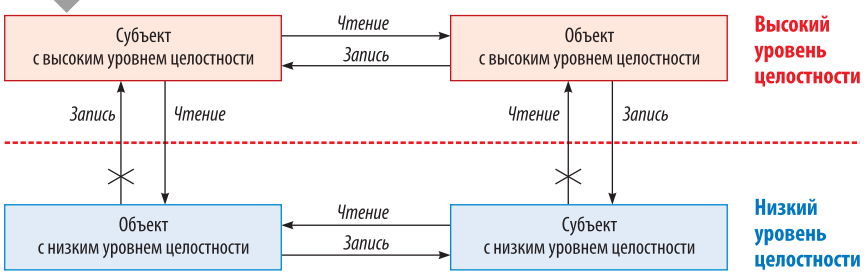


Рис. 2. ***Модель целостности Биба***

В основу следующего принципа контроля целостности данных заложен ряд идей, призванных обеспечить эффективное применение имеющихся механизмов обеспечения безопасности. На практике зачастую оказывается, что предусмотренные в системе механизмы безопасности или используются некорректно, или полностью игнорируются системными администраторами.

Простота использования защитных механизмов подразумевает, что самый безопасный путь эксплуатации системы будет также наиболее простым, и наоборот, самый простой – наиболее защищенным.

На практике наиболее часто употребляются две модели обеспечения целостности данных: модель целостности Кларка – Вильсона и модель Биба. Поскольку в АСУ проектирования кораблей используется мандатная модель, в дальнейшем будем рассматривать только модель Биба.

Модель Биба была разработана в 1977 году как модификация модели Белла –ЛаПадулы, ориентированная на обеспечение целостности данных. Аналогично модели Белла – ЛаПадулы, в ней используется решетка классов безопасности, трактуемых как решетка классов целостности (рис. 2).

Базовые правила модели Биба формулируются следующим образом:

1) простое правило целостности (Simple Integrity Property);

2) свойство (Star-Integrity Principle).

Для первого правила существует мнемоническое обозначение *No Read Down* (NRD): доступ на чтение дается, если уровень целостности (безопасности) объекта не ниже (или включает в себя) уровень целостности (безопасности) субъекта, а для второго – *No Write Up* (NWU): доступ на запись дается, если уровень целостности (безопасности) субъекта не выше (или включает в себя) уровня целостности (безопасности) объекта. Следовательно, состояние системы будет целостным тогда и только тогда, когда оно безопасно по чтению и записи.

Отдельного комментария заслуживает вопрос, что именно в модели Биба понимается под уровнями це-

лостности. Действительно, в большинстве приложений целостность данных рассматривается как некое свойство, которое либо сохраняется, либо не сохраняется, и введение иерархических уровней целостности может представляться излишним. В действительности уровни целостности в модели Биба стоит рассматривать как уровни достоверности, а соответствующие информационные потоки – как передачу информации из более достоверной совокупности данных в менее достоверную и наоборот. То есть модель Биба основывается на следующих допущениях: чем выше уровень безопасности объекта, тем выше его достоверность, и чем выше уровень безопасности субъекта, тем более достоверную информацию он может вносить в систему.

Формальное описание модели Биба полностью аналогично описанию модели Белла – ЛаПадулы. К достоинствам модели Биба следует отнести ее простоту, а также использование хорошо изученного математического аппарата. В то же время модель сохраняет все недостатки, присущие модели Белла – ЛаПадулы.

Выводы

При создании перспективных систем защиты рабочей среды СУБД на автоматизированных рабочих местах и серверах базы данных должны быть сняты ограничения существующих методов защиты [3]. Перечислим данные ограничения:

- не рассматриваются вопросы сопряжения с ГосСОПКа;
- не проработаны вопросы анализа запросов систем обнаружения вторжений к базам данных, не разработаны шаблоны;
- отсутствуют теория и нормативно-методический аппарат анализа защищенности БД от целенаправленных воздействий;
- существует только общая теория для информационных систем в целом;
- нет модели защищенной обработки транзакций в БД;
- существующие модели и механизмы управления безопасностью нацелены только на защиту данных;
- существующие критерии эффективности не учитывают целенаправленных воздействий;
- мониторинг компьютерных атак при взаимодействии с ГосСОПКа не описан в открытой литературе;
- противодействие компьютерным атакам на СУБД описывается только с точки зрения криптографической защиты данных;
- требуется разработка моделей, адаптированных к определенным структурам и алгоритмам функционирования СУБД.

Таким образом, выявлено противоречие между недостаточными техническими возможностями средств защиты СУБД по выявлению и нейтрализации атак в условиях целенаправленных воздействий и высокими требованиями к защищенности и своевременности обработки данных в СУБД на основании как ведомственных, так и общероссийских требований.

Для создания эффективной системы мониторинга требуется модернизация модели Биба путем введения правила «Без мандата нет изменения правил (грамматик) исполнения со всех уровней для внешнего поступления кода» [4].

Это означает необходимость блокирования как системных, так и прикладных процессов, которые не могут быть проконтролированы из запускаемой СУБД. А поскольку даже в защищенной отечественной СУБД «Линтер-ВС» такой механизм не реализован, для универсализации применения стоит включить в операционную систему данный механизм защиты среды выполнения прикладных процессов.

Заключение

Мониторинг защищенности работы СУБД SQL в АСУ проектирования корабля, с одной стороны, должен обеспечиваться за счет системы разграничения доступа на предмет отслеживания доступа оператора к объектам защиты, а с другой стороны, должна быть реализована система блокирования опасной функциональности, работающая на модифицированной в сторону ужесточения правил модели Биба.

Система мониторинга должна также фиксировать попытки параллельного с работой СУБД запуска неавторизованных процессов с последующей передачей этих данных на дальнейший анализ в аккредитованные ФСТЭК России испытательные лаборатории с целью выявления недекларируемых возможностей в выявленных исполнимых файлах.

Программная модель была разработана в интересах Национальной технической инициативы «Сейфнет» и предложена к реализации в виде программного комплекса, который должен также обеспечивать защиту работы СУБД в случае наличия закладок в операционной системе или осуществления хакерских действий по сети с удаленного компьютера в отношении рабочего места оператора. Ее практическая применимость апробирована на площадке киберполигона ИТЦ «Ингрия» (Санкт-Петербург) в 2022 году. Применение предложенной технологии защиты позволяет сделать следующий шаг к требуемым системам безопасности значимых объектов КИИ. ■

Автор выражает признательность заведующему кафедрой «Информационная безопасность» СПбГЭТУ «ЛЭТИ», д. т. н., доценту Е. Г. Воробьеву за оказанную им помощь в выполнении исследования и за критические замечания, высказанные в процессе подготовки настоящей статьи.

ЛИТЕРАТУРА

1. Буйневич М. В., Олауде А. Д. Состав и содержание элементов модели оценки устойчивости и безопасности ТКС // Актуальные проблемы информационной безопасности: сб. науч. трудов. – СПб.: СПбГИЭУ. – 2012. – С. 204–207.

2. Скакун В. В. Защита информации в базах данных и экспертных системах: пособие для студентов фак. радиофизики и комп. технологий. – Минск: БГУ. – 2015. – 140 с.

3. Воробьев Е. Г., Воробьева Д. Е. Безопасное функционирование инфраструктуры телерадиовещания в аспекте влияния на цифровую экономику // Защита информации. Инсайд. – 2023. – № 1 (109). – С. 2–6.

4. Воробьев Е. Г., Воробьева Д. Е. Модели оценки киберустойчивости транзакций в СУБД // Защита информации. Инсайд. – 2022. – № 6 (108). – С. 67–70.

Современные подходы к конструированию и использованию радиолокационных систем акустической разведки в США

УДК 621.382.2

Изложены современные подходы к конструированию радиолокационных систем акустической разведки (РЛСАР) в США. Приведены технические характеристики стоящих на вооружении американских спецслужб систем разведки. Описаны особенности формирования сигналов в закладочных устройствах.

Ключевые слова: АО «Лаборатория ППШ», радиолокационная система акустической разведки (РЛСАР), защита информации, технические средства разведки

Андрей Владимирович Лысов,
кандидат технических наук, доцент, заместитель генерального директора по научной работе
laser@pps.ru
АО «Лаборатория ППШ»

En **Modern Approaches to the Design and Use of Acoustic Reconnaissance Radar Systems in the USA**

A. V. Lysov,
PhD (Eng.), Associate Professor
laser@pps.ru
JSC «PPS Laboratory»

Modern approaches to the design of acoustic reconnaissance radar systems (ARRS) in the USA are outlined. The technical characteristics of the reconnaissance systems in service with the American intelligence services are given. The features of signal formation in stowing devices are described.

Keywords: JSC «PPS Laboratory», acoustic reconnaissance radar system (ARRS), information security, intelligence equipment

Настоящая статья продолжает цикл работ о применении радиолокационных систем акустической разведки (РЛСАР) [1–6].

К началу 1970-х годов разведки основных государств перешли к применению полуактивных электронных схем в конструкции закладочных устройств (ЗУ). Энергия внешнего высокочастотного воздействия больше не использовалась для электропитания микрофонного усилителя и модулятора. За счет этого технического решения удалось существенно снизить мощность зондирующего сигнала [6, 7]. Именно подобные системы активно применялись до начала 1990-х, но американцам, например, было понятно, что такой демаскирующий признак, как наличие исходного акустического сигнала в эфире, раскрывает факт применения РЛСАР по конкретному объекту. Использование относительно простой схемы с поднесущими частотами стала считаться явно недостаточной, так как легко вскрывалась при радиоконтроле.

Например, еще в 1958 году, по заданию ГРУ ГШ ВС СССР, был разработан переносной радиоприемник Р-375 «Кайра-МА» с диапазоном частот от 20 до 500 МГц и чувствительностью в АМ-режиме – не хуже 4 мкВ. В состав изделия входило анализирующее устройство (блок) Р-375-А (рис. 1), позволявшее исследовать (прослушивать) принимаемый

сигнал в спектре частот 4…330 кГц с выделением 1–2 боковых полос. Приемник уже в 1960-е годы позволял даже слабо подготовленному оператору успешно решать задачи радиоконтроля, в том числе в режиме прослушивания поднесущих [8].

В этот период на вооружении ЦРУ появилось достаточно много радиозакладок, в которых применялись сложные виды модуляции для маскировки исходного речевого сигнала, например, SRT-52, SRT-91, SRT-107 и т. д. Наиболее приемлемым для работы на тот момент был выбран частотный диапазон 1…2 ГГц. Логично, что по этому же пути развивались в дальнейшем и ЗУ из комплекта РЛСАР.

В настоящее время в разведсообществе США работа по интересующему нас направлению продолжается, но уже без участия ЦРУ. Применение РЛСАР при проведении операций за рубежом, предположительно, признано слишком опасным. Однако «упавшее знамя» подхватили в Агентстве национальной безопасности (АНБ) – подразделении Министерства обороны США, которое входит в состав Разведывательного сообщества на правах независимого разведывательного органа и занимается радиоэлектронной разведкой и защитой электронных коммуникационных сетей американских госучреждений. Современные полуактивные РЛСАР подкупают низкой стоимостью эндовибратора и использованием стандартного (недорогого) оборудования для облучения и приема. Рассмотрим относительно современные системы, используемые АНБ США.

Широко распространенным является семейство радиолокационных ретрорефлекторов из набора «Angryneighbour» (дословно – «злой сосед»). При включении радар создает в целевой области поле высокой мощности на выбранной частоте. Информативный сигнал с радиозакладки модулирует этот отраженный от антенны ЗУ сигнал, а приемный блок РЛСАР считывает промодулированный сигнал и с помощью фильтра выделяет из него информативный сигнал. Радар в этой схеме как бы организует канал связи между ЗУ и приемной антенной. Использование мощного внешнего несущего сигнала по-прежнему имеет ряд преимуществ:

- размеры антенны и требования к модулю «излучения» (аналогу передатчика) закладки могут быть сведены к минимуму;
- полуактивная закладка будет потреблять значительно меньше энергии, чем обычный радиомикрофон (следовательно, размер батарейного блока можно также уменьшить);
- закладка «включается» только при облучении ее сигналом определенной частоты, следовательно, выявить ее несколько сложнее, чем обычную радиозакладку.

В качестве приемо-передающего устройства РЛСАР используется портативный радар CTX4000 (рис. 2), который работает в диапазоне 1…2 ГГц. Мощность внутреннего усилителя составляет 2 Вт, внешнего – до 1 кВт. С 2009 года CTX4000 постепенно заменялся на более современную версию Photoanglo размером с небольшой портфель, но с расширенным до 4 ГГц диапазоном частот. Отметим, что стоимость радара Photoanglo – 40 000 долл. Характеристики радаров приведены в таблице [9, 10].

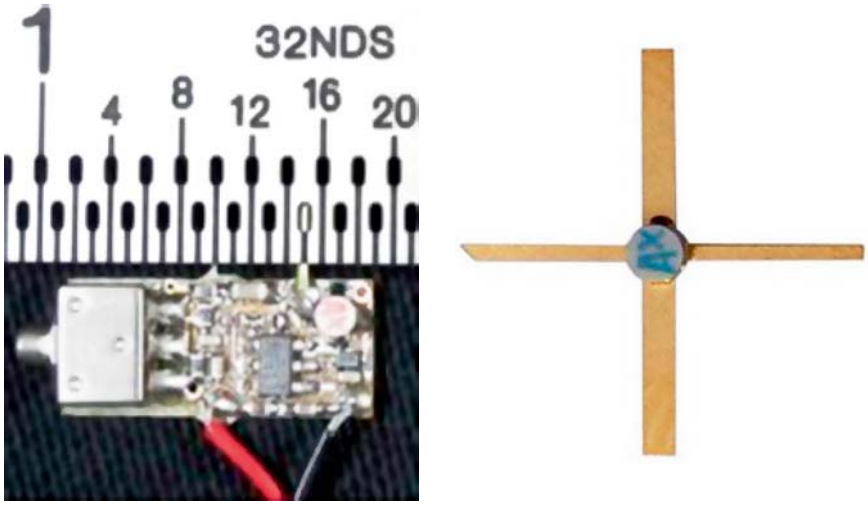
Photoanglo – это совместный проект АНБ и GCHQ (*Government Communications Headquarters*) по разработке радиолокационной системы следующего поколения [7]. Напомним, что GCHQ – Центр правительственной связи Великобритании – спецслужба, ответственная за ведение радиоэлектронной разведки и обеспечение защиты информации органов правительства и армии. Она входит в состав Объединенного раз-

Рис. 1. ***Радиоприемник Р-375 (сверху – блок Р-375-А)***

Рис. 2. ***Портативный радар CTX4000***

Таблица. ***Характеристики радаров РЛСАР АНБ США***

Параметр	Тип радара	
	CTX4000B	Photoanglo
Диапазон, ГГц	1…2	1…4
Полоса пропускания, МГц	45	450
Вид излучения	Непрерывное	Непрерывное
Максимальная выходная мощность, Вт	2	2
Максимальная выходная мощность с внешним усилителем , Вт	1000	-
Наличие регулируемых ВЧ- и НЧ-фильтров	+	-
Ручная фазовая подстройка	+	-
Дистанционное управление	+	+
Выходы: ● видео; ● питания внешнего предусилителя приемника; ● передающей антенны	 + + +	 + – +
Входы: ● антенны приемника; ● внешнего генератора	 + +	 + +
Масса, кг	Нет данных	4,5



а *б*

Рис. 3. ***Полуактивный эндовибратор Loudauto (а) и полевой транзистор Mitsubishi MGF1302 (б), маркировка которого – Ax – хорошо видна в правом верхнем углу платы***

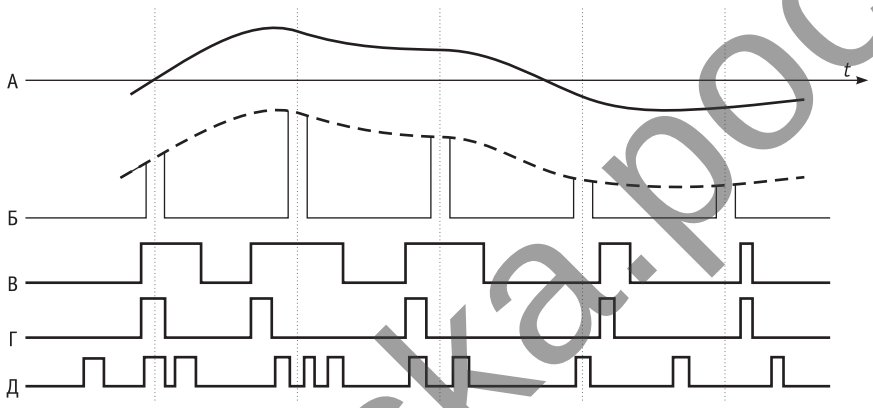


Рис. 4. ***Осциллограммы исходного аналогового сигнала (а) после его преобразования в амплитудно-импульсную (б), широтно-импульсную (в) и импульсно-позиционную модуляции (г)***

ведывательного комитета, совместно с MI5 (внутренняя разведка) и MI6 (внешняя разведка).

РЛСАР Photoanglo использует внешние антенны разных типов – рупорные, спиральные, параболические, логопериодические. Часть сигнала передатчика используется в качестве гетеродина приемника. К видеовыходу РЛСАР рекомедуется подключать стандартное оборудование. Это сделано в рамках программы использования в спецтехнике COTS equipment (*Commercial Off-The-Shelf* – готовые к применению), то есть оборудования, изготовленного с максимальным использованием коммерчески доступных элементов. Внедрение в специальные устройства коммерческих компонентов широкого назначения позволяет получать практически неограниченные возможности модернизации, наращиваний и расширений для удовлетворения перспективных требований. В первую очередь, это касается применения различных видов модуляции принимаемых сигналов.

Рассмотрим полуактивный эндовибратор из семейства Angryneighbour с кодовым названием Loudauto, разработанный ранее 2007 года в АНБ США.

Чувствительный микрофон EK/EY (коммерческий микрофон компании Knowles для слуховых аппаратов стоимостью около 10 долл.) позволяет прослушивать «офисный» разговор с расстояния более 6 м. ЗУ работает от 3-вольтовой батарейки и потребляет настолько мало энергии, что токи саморазряда батареи могут быть больше токов потребления ЗУ. По этому признаку традиционно относим его к полуактивным. Микрофон собран из широкодоступных на рынке компонентов, поэтому при обнаружении его будет трудно связать с высокотехнологичной продукцией АНБ (отсюда и несколько «кустарный» вид (рис. 3 [9])).

Устройство активируется (облучается) сигналом на частоте от 1 до 2 ГГц с поста прослушивания. Аналоговое аудио с микрофона (рис. 4*а*) преобразуется в цифровой сигнал с импульсно-позиционной модуляцией (*Pulse Position Modulation*, PPM). Напомним, что PPM – это форма модуляции сигнала, в которой M битов сообщения кодируются путем передачи одного импульса в один из 2^M возможных требуемых временных сдвигов. PPM (рис. 4*г*) можно рассматривать как частный случай широтно-импульсной модуляции (*Pulse Width Modulation*, PWM) (рис. 4*в*) [7].

PPM широко используется в коммерческих продуктах, например, для связи с бесконтактной смарт-картой ISO/IEC 15693, а также для реализации ВЧ-протокола электронного кода продукта класса 1 для RFID-меток. Комплектующие для таких устройств можно купить за 1000 руб. на Aliexpress. По косвенным признакам, ЦРУ применяло радиомикрофоны с PPM-модуляцией уже в 70-е годы прошлого века [7].

PPM-сигнал модулируется по частоте (в соответствии с ГОСТ Р ИСО/МЭК 15693-3-2011, требуется использовать одну или две поднесущие частоты [12]). Переизлученный сигнал принимается на посту прослушивания, где, как правило, расположены изделия Photoanglo, и далее обрабатывается с помощью COTS-оборудования. Так, демодуляция и дальнейшая обработка сигнала осуществляется посредством коммерческого портативного анализатора спектра, например, Rohde & Schwarz FSH (рис. 5) [9].

Во многом Loudauto можно рассматривать как дальнейшее развитие программы ЦРУ Easychair [4–6] в части применения полуактивных ЗУ в сочетании с более совершенными радиомикрофонами серии SRT, которые использовали PPM-модуляцию.

Варианты реализации изделия были самыми разными. Например, «тройной импульс» – метод маскировки, основанный на PPM, который активно использовался в ЦРУ и получил название «тип-52». Принцип его работы следующий. Система фиксирует «образцы» звука на случайных интервалах (под управлением генератора шума) и преобразует их в PPM. На приведенной на рис. 6 временной диаграмме случайные выборки показаны темно-серым цветом (T1, T2 и T3). Каждый импульс находится в пределах двух опорных импульсов (светло-серый цвет) с фиксированным временным расстоянием *d* между собой. Каждый импульс имеет одинаковую ширину и амплитуду. Фактический аудиосигнал определяется (восстанавливается) по позиции темно-серого импульса по отношению к двум светло-серым опорным импульсам.

Другой вариант схемы маскировки, также основанный на PPM, в ЦРУ был известен как «тип-56» или «вырезанные импульсы» (Rejected Pulse). В этой схеме импульсы формируются через фиксированные временные интервалы *i* (рис. 7). По закону генератора шума, до пяти последовательных импульсов (показаны светло-серым цветом на рис. 7) отбрасываются (не передаются), что внешне приводит к виду «хаотической импульсной последовательности». Относительное положение каждого из оставшихся импульсов несет информацию о модуляции. Сигнал можно восстановить только в специальном совместимом приемнике.

Каждый импульс имеет длительность порядка 0,5 мкс (полоса $f_c \approx 1$ МГц). При этом ширина полосы сигнала на поисковом анализаторе спектра может достигать 100 МГц при размещении антенны в непосредственной близости от ЗУ (рис. 8) [9].

На рис. 9 представлено предположение о том, как работает устройство Loudauto. Слева находится стандартный миниатюрный микрофон с встроенным предварительным усилителем. Аналоговый сигнал от микрофона подается на вход импульсного позиционного модулятора (PPM), который, возможно, программно реализован в небольшом промышленном стандартном контроллере AVR [13].

Очевидно, что в приведенной на рис. 9 схеме не хватает аналога хорошо отработанных в США методов типа «вырезанные импульсы», «тройной импульс» и им подобных применительно к стандартным устройствам ЦРУ. Кроме того, здесь отсутствует частотный модулятор (предполагается использование поднесущей с частотой порядка 100…500 кГц). Полевой транзистор *(Field-Effect-Transistors*, FET) явно используется как ключ. Надо отметить, что Loudauto имеет приемлемый размер (без элементов питания – примерно 1,5 см в длину) и потрясающе низкую для ЗУ цену – 30 долл. [9].

В целом, Loudauto выглядит как довольно примитивный вариант полуактивных (полупассивных) RFID-

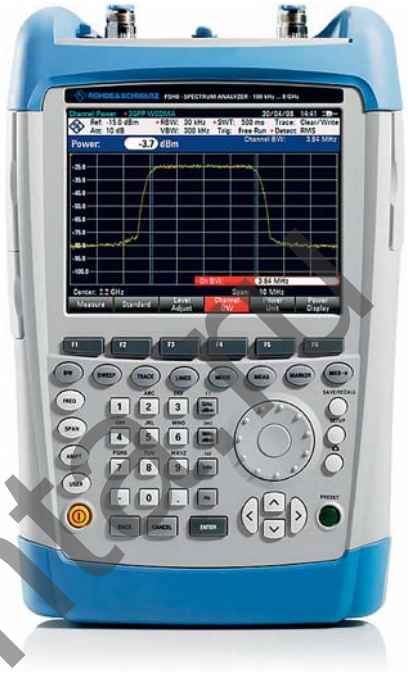


Рис. 5. ***Портативный анализатор спектра R&S FSH [11]***

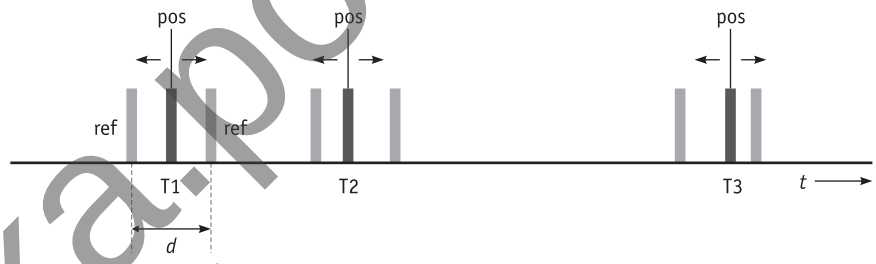


Рис. 6. ***Временна́я диаграмма метода маскировки «тройной импульс»***

Рис. 7. ***Временна́я диаграмма метода маскировки «вырезанные импульсы»***

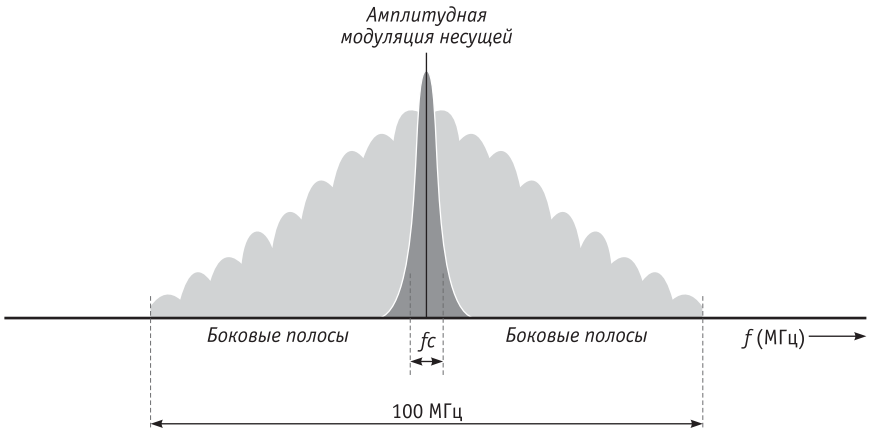


Рис. 8. ***Спектр PPM-модулированного сигнала (любого типа) в ближней зоне [9]***

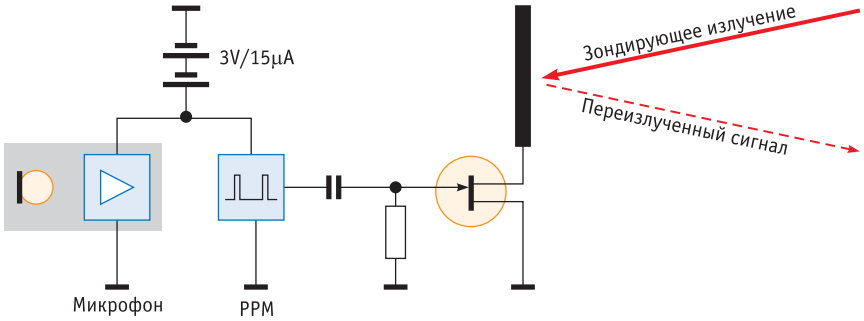


Рис. 9. ***Предполагаемая блок-схема ЗУ Loudauto***

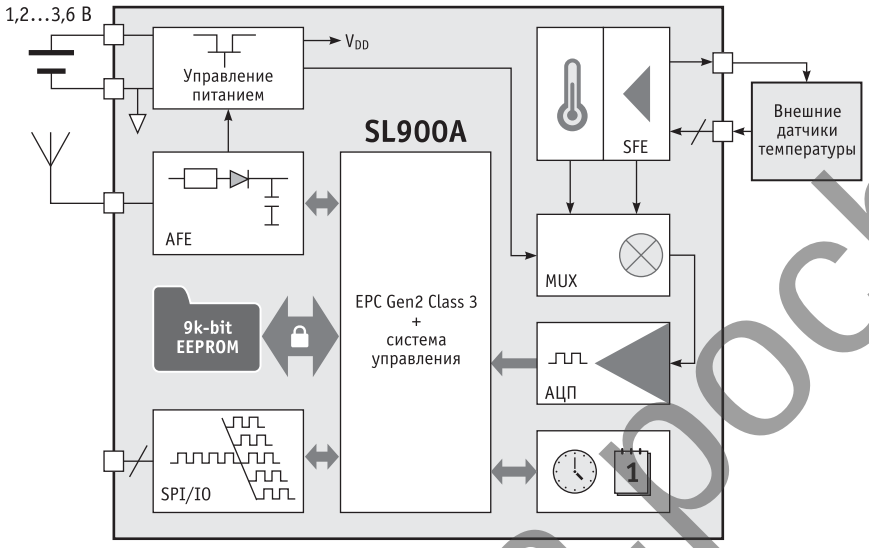


Рис. 10. ***Структурная схема SL900A [14]***

меток, широко распространенных в различных отраслях. Напомним, что RFID (*Radio Frequency IDentification*, радиочастотная идентификация) – это способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках. Для работы на дистанции более 10 м эти изделия обычно настроены в диапазоне около 900 МГц, но точная рабочая частота зависит от настройки приемной антенны RFID. В нашем случае проблемы с согласованием антенны (кусок провода) нет, поэтому работа на частоте свыше 1 ГГц для попадания в диапазон РЛС СТХ4000В или Photoanglo не является проблемой.

Ввиду роста возможностей коммерческих RFID-транспондеров, они уже являют собой не только пассивные, но и полноценные активные и полуактивные датчики, которые благодаря собственному источнику питания обладают даже некоторыми «интеллектуальными» способностями. Последний вариант стандарта RFID подразумевает наличие нескольких классов меток, отличающихся применяемым диапазоном радиочастот и коммуникационными способностями:

- Class 0 – пассивные метки с диапазоном UHFl, программируемые на этапе производства;
- Class 1 – пассивные метки с диапазонами UHF и HF с возможностью однократного программирования;
- Class 2 – пассивные метки с возможностью многократного программирования;
- Class 3 – многократно программируемые пассивные и полупассивные датчики с возможностью записи различных параметров;
- Class 4 – многократно программируемые активные транспондеры, имеющие собственные передатчики и способные самостоятельно взаимодействовать с другими RFID-метками и считывателями;
- Class 5 – транспондеры, обладающие не только всеми особенностями предыдущего класса, но и способные снабжать питанием другие метки, а также обеспечивать обмен данными со считывателями и другими устройствами.

Очевидно, что RFID-метки, начиная от Class 3 и выше, – это достаточно сложные устройства, при этом их довольно просто реализовать путем применения готовых микросхем, например, SLA900A от компании AMS. SLA900A – высокоинтегрированный чип RFID-метки, соответствующий требованиям EPC Gen2 Class 3. Он предназначен для создания пассивных и полупассивных RFID-транспондеров Class 3 диапазона UHF (860…960 МГц), использующих для питания либо энергию радиоизлучения (пассивная версия), либо собственный аккумулятор. С помощью SL900A можно создавать:

- пассивные RFID-метки;
- пассивные и полупассивные RFID-датчики с питанием от радиоизлучения;
- пассивные и полупассивные RFID-датчики с питанием от аккумулятора и функцией накопления данных;
- пассивные и полупассивные RFID-датчики с управляющим микроконтроллером и питанием от аккумулятора.

При этом главная прелесть SL900A состоит в том, что для каждого из перечисленных приложений потребуется минимум внешних компонентов, так как «на борту» SL900A есть все необходимое:

- ядро, отвечающее за реализацию RFID-интерфейса;
- система управления и взаимодействия с внешним контроллером по SPI;
- аналоговые цепи для подключения внешних датчиков;
- система управления питанием.

По этой причине для создания простейшего датчика (рис. 10) потребуются всего лишь внешняя антенна (провод) и, в полуактивном варианте, аккумулятор.

Если внешние датчики температуры заменить на микрофон, то получится вполне приличное ЗУ с гораздо большими, чем у Loudauto, возможностями. Отметим, что SL900A далеко не самая «интелектуальная»

микросхема. Повышение частотного диапазона РЛС до 4 ГГц позволяет АНБ применять огромное разнообразие RFID-датчиков, работающих в диапазоне 2,4 ГГц, которые имеются на коммерческом рынке. По мнению автора, американская разведка просто не может не воспользоваться такой возможностью расширить арсенал ЗУ, тем более что из-за обилия различных источников радиоизлучения в данном радиодиапазоне довольно просто «спрятаться».

Напомним, что кроме Loudauto в комплект семейства устройств Angryneighbour входят и другие изделия, назначение которые формально выходит за пределы настоящей статьи. Их можно отнести к средствам радиотехнической разведки или (в меньшей степени) к разведке побочных электромагнитных излучений.

АНБ совместно с ФБР продолжают активно использовать радиолокационные устройства разведки на национальной территории США. Доподлинно известно о проведении подобных операций в отношении более 28 дипломатических представительств в Вашингтоне и Нью-Йорке [15]. Интересно отметить, что в отношении дипломатических представительств Великобритании, Германии, Китая и России методы зондирования высокочастотными сигналами возможно внедренных туда ЗУ в последние десятилетия американцы не применяли, считая, предположительно, такие операции достаточно рискованными ввиду относительно несложного выявления факта наличия ЗУ. ■

ЛИТЕРАТУРА

1. Лысов А. В. Общая классификация активных методов акустической разведки // Защита информации. Инсайд. – 2022. – № 4 (106). – С. 45–49.

2. Лысов А. В. Первый случай применения средства акустической разведки с использованием метода высокочастотного зондирования // Защита информации. Инсайд. – 2022. – № 5 (107). – С. 82–88.

3. Лысов А. В. Оценка технических характеристик РЛСАР с использованием акустически возбужденных пассивных резонаторов // Защита информации. Инсайд. – 2022. – № 6 (108). – С. 71–78.

4. Лысов А. В. Причины отказа от применения в США и РЛСАР с использованием пассивных эндовибраторов // Защита информации. Инсайд. – 2023. – № 1 (109). – С. 43–48.

5. Лысов А. В. Технические причины перехода от механических резонаторов к пассивным электронным закладочным устройствам в радиолокационных системах акустической разведки // Защита информации. Инсайд. – 2023 – № 6 (114). – С. 22–26.

6. Лысов А. В. Повышение эффективности радиолокационных систем акустической разведки путем использования полуактивных закладочных устройств // Защита информации. Инсайд. – 2024. – № 1. – С. 27–31.

7. Лысов А. В. Электромагнитное зондирование акустически возбужденных объектов (радиолокационные системы акустической разведки). – СПб.: Медиапапир. – 2020. – 678 с.

8. Анализирующее устройство Р-375-А. Краткое описание и инструкция по эксплуатации. ТЦ2.770.502 ТО.

9. NSA ANT catalog [Электронный ресурс]. – URL: https://nsa.gov1.info/dni/nsa-ant-catalog/keyboards/index.html (дата обращения: 12.12.2024).

10. Price [Электронный ресурс]. – URL: https://yandex.ru/images/search?text= PHOTOANGLO&stype=image&lr=2&source=wiz&pos=13&img_url=https %3A %2F %2Fcryptome.org %2F2014 %2F01 %2Fnsa-codenames-03.JPG&rpt=simage/ (дата обращения: 12.12.2024).

11. Портативный анализатор спектра R&S®FSH [Электронный ресурс]. – URL: https://www.rohde-schwarz.com/ru/product/fsh-productstartpage_63493-8180.html (дата обращения: 12.12.2024).

12. ГОСТ Р ИСО/МЭК 15693-3-2011. Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты удаленного действия. Часть 3. Антиколлизия и протокол передачи данных (утв. и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 13 декабря 2011 года № 1000-ст).

13. Loudauto [Электронный ресурс]. – URL: https://www.cryptomuseum.com/ covert/ bugs/nsa-ant/loudauto/index.htm (дата обращения: 12.12.2024).

14. 1SL900A [Электронный ресурс]. – URL: https://www.rlocman.ru/review/article.html?di=164226/ (дата обращения: 12.12.2024).

15. Лысов А. В. Компрометирующие излучения. Том 1. История и современное состояние защиты информации от компрометирующих излучений. – СПб.: Медиапапир. – 2022. – 498 с.

Уровни доверия идентификации и аутентификации при удаленном электронном взаимодействии

Методическое пособие

В пособии приведена методология построения иерархии уровней доверия к результатам идентификации и аутентификации субъектов доступа, в том числе при удаленном электронном взаимодействии. На основе разработанных и модернизированных моделей и методов исследования процессов идентификации и аутентификации предложены методики формирования уровней доверия к результатам идентификации и аутентификации для информационных систем различного назначения.

Перечислены способы достижения определенных уровней доверия к результатам идентификации и аутентификации.

Проведенный анализ процесса идентификации субъектов доступа позволяет применять полученные научные результаты на стадиях проектирования и эксплуатации систем идентификации и аутентификации, что допускает возможность существенного сокращения сроков проектирования и/или модернизации существующих информационных систем с учетом требований безопасности, надежности и достоверности идентификации.

Ознакомиться с подробным содержанием пособия и оформить заказ можно на сайте www.inside-zi.ru

Мультимодальный подход к обнаружению объектов на видео- и тепловизионных данных при помощи сверточной нейросети

УДК 004.93

Представлен мультимодальный подход к обнаружению объектов на основании данных теле- и тепловизионного видеопотока. Цель исследования состоит в проверке возможности и целесообразности использования многоканального обучения сверточных нейросетей в задачах распознавания объектов на видео. Для достижения поставленной цели использовались методы компьютерного моделирования, машинного обучения, глубоких аналогий, в результате чего была разработана структура модели машинного обучения и распознавания объектов видеопотока. Теоретическим выводом исследования является алгоритм обучения и распознавания, практическим – архитектура модели в программном коде.

Ключевые слова: обнаружение объектов, сверточные нейронные сети, машинное обучение, компьютерное зрение, многоканальное обучение

Надежда Валерьевна Братусь
bratus@mirea.ru

Сергей Владимирович Маличенко
malichenko.mirea@bk.ru

Владимир Александрович Мордвинов,
кандидат технических наук
mordvinov@mirea.ru

МИРЭА – Российский технологический университет

Введение

Процедура обнаружения объектов выполняется в основном для автоматического анализа изображений в системах наблюдения. Возможности использования компьютерного зрения приобрели свою популярность благодаря уникальной способности производить анализ изображений быстро, на протяжении длительного времени и в многозадачном режиме. Одновременная фиксация окружающей обстановки и композитный анализ повышают точность результатов выявления объектов на кадре [1].

В настоящее время для реализации алгоритмических методов машинного обучения и распознавания используют специальные фреймворки: библиотеки с заранее подготовленными наборами исходных данных и весами. Среди имеющихся широко распространены TensorFlow, PyTorch, OpenCV из-за наличия в своем составе готовых решений по составлению потоков данных и архитектуры сети. Абстрагирование от программно-аппаратной платформы позволяет использовать их на множестве устройств без адаптации к конкретным операционным системам.

En

Multimodal Approach to Object Detection in Video and Thermal Imaging Data Using Convolutional Neural Network

N. V. Bratus
bratus@mirea.ru

S. V. Malichenko
malichenko.mirea@bk.ru

V. A. Mordvinov,
PhD (Eng.)
mordvinov@mirea.ru

MIREA – Russian Technological University

A multimodal approach to object detection based on tele- and thermal imaging video stream data is presented. The purpose of the study is to test the possibility and feasibility of using multi-channel training of convolutional neural networks in object recognition tasks on video. To achieve this goal, methods of computer modeling, machine learning, and deep analogies were used. The result is the developed structure of the machine learning model and object recognition of the video stream. The theoretical conclusion is the learning and recognition algorithm, the practical one is the architecture of the model in the program code.

Keywords: object detection, convolutional neural networks, machine learning, computer vision, multi-channel learning

а *б* *в*

Рис. 1. ***Исходный набор данных: а) RGB-изображение; б) термограмма; в) аннотированная термограмма***

Представленная статья описывает результат исследований, направленных на создание модели по распознаванию объектов на основе двух потоков данных: видео- и тепловизионного потока. Инициатива по созданию подобной модели обусловлена отсутствием имеющихся готовых реализаций многоканального распознавания с приемлемой точностью. Большинство примеров работ [2–5] связаны с распознаванием объектов на основе теле- или тепловизионного потока [6, 7] по отдельности с последующей обработкой распознанных данных. Исследование [8] сводится к отысканию движущихся объектов с использованием Гауссовой смеси распределений и алгоритма LMEDS для определения объектов потока. В статье [10] для распознавания и проведения предварительного дискриминативного обучения и более точной классификации действий объекта в кадре задействованы глубокие сверточные сети (ConvNets).

Метод многоканального обучения и распознавания позволяет повысить точность обработки данных задействованием при оценке нескольких источников гетерогенной информации. Этот подход использует данные с положительной корреляцией, обусловленной наличием определенной взаимосвязи, которая зачастую сложна для математического описания, но может быть использована в качестве базового набора.

Описание алгоритма

Исходным набором для проведения обучения стал FLIR Thermal Starter Dataset [6], который содержит RGB-изображения, термограммы в бело-сером спектре (рис. 1) и файл аннотаций в формате MSCOCO. При проведении процесса обучения были использованы размеченные данные тепловизионных карт.

Для более адекватной адаптации алгоритма распознавания предполагается наличие RGB-изображения с временной меткой, аналогичной термограмме. В таком случае совмещение кадров произойдет с минимальными расхождениями в окружении, и станет возможным достижение более высокой точности результатов. Для обучения была задействована специализированная сверточная нейронная сеть YOLO, использующая технологии локализации и классификации объектов на изображении за один прямой проход по сети, что позволяет задействовать ее в режиме реального времени.

Предварительно был подготовлен набор данных на основе исходных совмещенных изображений. Алгоритм совмещения представлен на врезке 1, где *frame_rgb* – кадр RGB, frame_tcm – кадр термограммы.

Используя функцию addWeighted библиотеки OpenCV 2, удалось реализовать наложение изображений, при котором ½ кадра составляет RGB и ½ – ТСМ. Результат наложения представлен на рис. 2.

Очевидно, что совмещение кадров имеет определенную долю неточности, которая вызвана разрешением, временем экспозиции, углом обзора камеры и тепловизора. Для уменьшения шумов на потоковых данных рекомендуется адаптивно менять фокусировку на каждом объективе. Их близкое расположение уменьшает объемный эффект на плоскости и снижает рассеивание на границах объектов. Код алгоритма обучения по имеющимся аннотациям представлен на врезке 2.

На начальном этапе производится импорт модели YOLO из пакета *ult-*

Врезка 1

Алгоритм совмещения

```
gray_frame_rgb = cv2.cvtColor(frame_rgb, cv2.COLOR_BGR2GRAY)
gray_frame_tcm = cv2.cvtColor(frame_tcm, cv2.COLOR_BGR2GRAY)

alpha = 0.5
beta = 1 – alpha

# Наложение изображений
result = cv2.addWeighted(gray_frame_rgb, alpha, gray_frame_tcm, beta, 0)
```

Врезка 2

Алгоритм обучения

```
from ultralytics import YOLO

model = YOLO("yolov8n.pt")

if __name__ == '__main__':
  results = model.train(data="config.yaml", epochs=3, show=True, device=0)
```

Рис. 2. ***Наложение кадров RGB и TCM***

ralytics. Далее производится инициализация модели конфигурационным файлом. Процесс обучения запускается вызовом метода *train* объекта *model*. В аргументах передается файл конфигураций *yaml*, где указаны пути к директориям с изображениями, количество эпох обучения и флаг для вывода отладочной информации. Для ускорения был собран PyTorch с возможностью использования GPU и CUDA v11. Весь процесс обучения выполнялся на NVIDIA Jetson Xavier NX и занял около 11 минут. Далее полученные весы были задействованы в распознавании объектов совмещенных видеопотоков.

Распознавание

По схожей аналогии осуществляется процесс распознавания. Схематично реализация архитектуры представлена на рис. 3.

Изначально следует подготовить видеопоток. Основная проблема на данном этапе заключается в различии показателей FPS (*frames per second* – кадры в секунду) камеры и тепловизора, что ограничивает выборку исходных кадров. Для устранения данного несоответствия производится синхронизация изображений с выделением кадра в равные промежутки времени из видео- и тепловизионного потока. Далее происходит выборка кадров с последующей нормализацией, после чего осуществляется слияние кадров и формирование видеопотока для распознавания нейросетью. Алгоритм распознавания представлен на врезке 3.

После инициализации модели внутри вызова *main* осуществляется запуск процесса детектирования. В качестве аргументов передается адрес RTSP-потока после слияния кадров и флаг *show* для вывода результата на экран. Кадр потока распознавания представлен на рис. 4.

Точность определения объектов практически совпадает с исходной аннотацией – 87 %. Явное преимущество такого подхода составляет наличие нескольких источников гетерогенных данных. Эффективность детектирования видео приемлема в дневное время суток или при свете, но существенно падает в отсутствие освещения. Тепловизионный поток позволяет устранить эти недостатки с помощью тепловой карты изображения.

Для проведения обучения исходные изображения должны быть определенным образом подготовлены и выверены по временным меткам, а именно, обладать одинаковыми VITC (*Vertical Interval Timecode*) кодами [9], что может привнести сложности при синхронизации источников видео. Кроме того, при наложении кадров изображения должны быть центрированы и иметь одинаковое разрешение, что весьма проблематично, так как зачастую источники рассинхронизированы и работают независимо друг от друга. На точность распознавания также влияет время экспозиции и глубина фокусировки, для более адекватного результата эти величины должны быть одинаковыми у обоих источников.

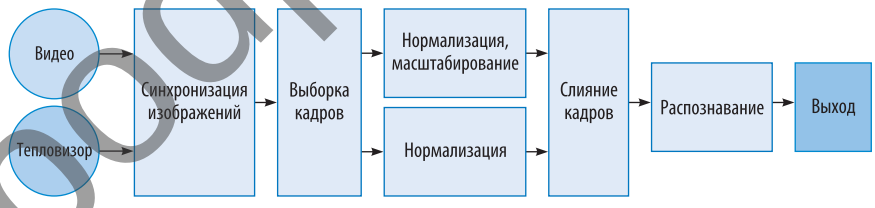


Рис. 3. ***Схема алгоритма распознавания***

Врезка 3

Алгоритм распознавания

```
from ultralytics import YOLO
weight_path = "best.pt"
model = YOLO(weight_path)
if __name__ == '__main__':
  results = model(source="rtsp://127.0.0.1:8554/video_stream", show=True)
```

Направления дальнейших исследований

В качестве вектора развития предложенной тематики можно рассмотреть применение источников данных, работающих на иных физических принципах.

LIDAR (*Light Detection and Ranging*) использует технологию испускания лазером волн оптического диапазона с дальнейшей регистрацией лазерных импульсов. В качестве третичного источника информации LIDAR позволит определять угловые координаты объектов [10]. Регистрация данных о поверхности значительно расширит объем начальных данных об окружающей обстановке и повысит точность распознавания.

Перспективным направлением станет использование, помимо оптического диапазона, еще и устройств, работающих на электромагнитных или акустических частотах спектра. Радар позволит определить рельеф поверхности при отсутствии видимости или теплометрических меток объекта, учесть направление и скорость движения [11].

Рис. 4. ***Результат процесса детектирования объектов***

Заключение

Представленная статья служит результатом проверки возможности использования многоканального обучения сверточных нейросетей при распознавании объектов на основе видео- и тепловизионного потока, что является современной научно-технической задачей. Предложенная схема распознавания может быть расширена добавлением новых источников обучения и анализа информации для проведения более точного процесса распознавания. Проработка гипотетических идей по модернизации алгоритма обучения также может быть реализована на основе представленной архитектуры. Инновационное внедрение многоканального обучения позволит повысить точность и объективность анализа информации, устранить множество проблем компьютерного зрения.

Вышесказанное позволяет утверждать, что авторская идея реализации задачи является актуальной и новаторской, а поставленные цели исследования достигнуты. ■

ЛИТЕРАТУРА

1. Акиншин Н. С. и др. К вопросу построения систем распознавания объектов многоканальными комплексами зондирования на основе нейронных сетей и фрактальных сигнатур // Радиотехника и электроника. – 2020. – Т. 65, № 7. – С. 705–713.

2. Leira F. S. et al. Object Detection, Recognition, and Tracking from UAVs Using a Thermal Camera // Journal of Field Robotics. 2021. V. 38, № 2. P. 242–267.

3. Shi Y., Wang N., Guo X. YOLOV: Making Still Image Object Detectors Great at Video Object Detection // Proc. of the AAAI Conference on Artificial Intelligence. 2023. V. 37, № 2. P. 2254–2262.

4. Cong R. et al. PSNet: Parallel Symmetric Network for Video Salient Object Detection // IEEE Transactions on Emerging Topics in Computational Intelligence. 2022. V. 7, № 2. P. 402–414.

5. Ingle P. Y., Kim Y. G. Real-Time Abnormal Object Detection for Video Surveillance in Smart Cities // Sensors. 2022. V. 22, № 10. P. 3862.

6. Jiang C. et al. Object Detection from UAV Thermal Infrared Images and Videos Using YOLO Models // International Journal of Applied Earth Observation and Geoinformation. 2022. V. 112. P. 102912.

7. Altay F., Velipasalar S. The Use of Thermal Cameras for Pedestrian Detection // IEEE Sensors Journal. 2022. V. 22, № 12. P. 11489–11498.

8. Szwoch G., Szczodrak M. (2013). Detection of Moving Objects in Images Combined from Video and Thermal Cameras // In: Dziech A., Czyżewski A. (eds) Multimedia Communications, Services and Security. MCSS 2013. Communications in Computer and Information Science, T 368. Springer, Berlin, Heidelberg. – DOI: 10.1007/978-3-642-38559-9_23.

9. Perek P., Mielczarek A., Makowski D. High-performance Image Acquisition and Processing for Stereoscopic Diagnostic Systems with the Application of Graphical Processing Units // Sensors. 2022. V. 22, № 2. P. 471.

10. Hasan M. et al. LiDAR-Based Detection, Tracking, and Property Estimation: A Contemporary Review // Neurocomputing. 2022. № 506. P. 393–405.

11. Wang Y. et al. RODNet: A Real-Time Radar Object Detection Network Cross-Supervised by Camera-Radar Fused Object 3D Localization // IEEE Journal of Selected Topics in Signal Processing. 2021. V. 15, № 4. P. 954–967.

НОВОСТИ

Что будет, если установить на смартфон 100 приложений и не пользоваться им трое суток?

Телефоны могут без ведома владельцев ежедневно передавать с неизвестной целью гигабайты данных в другие страны.

Эксперимент, проведенный журналистом издания Cybernews Эрнестом Наприсом, наглядно показал, что не стоит бездумно устанавливать приложения на свой смартфон, даже если они были загружены из официальных источников.

Наприс сбросил свой Android-смартфон до заводских настроек, а затем загрузил на него 100 самых популярных бесплатных приложений из Google Play Store. После запуска всех приложений и выдачи им требуемых разрешений, а также регистрации аккаунтов, где это требовалось для получения полного функционала, он оставил телефон на трое суток со включенным Интернетом и никак не взаимодействовал с ним все это время. Для отслеживания подключений весь трафик направлялся через частный DNS-сервис.

Эксперимент показал, что за три дня телефон осуществил 6296 DNS-запросов. Основная доля трафика пришлась на США, при том что сам автор исследования физически находился в Литве, и распределилась между тремя крупными технологическими компаниями: Google – 600 запросов. Facebook* – около 300 запросов, Microsoft – около 250 запросов. Кроме того, данные уходили и на американские серверы TikTok, причем по объему информации китайская платформа смогла обойти даже Google с показателем порядка 800 запросов.

Подключения к российским IP-адресам происходили не менее 39 раз, в основном к серверам Яндекса, хотя на смартфоне не было установлено приложений от этой компании, а к китайским (в основном к серверам Alibaba, Aliexpress и Taobao) – 15 раз. Кроме того, телефон трижды устанавливал связь с серверами во Вьетнаме, что лишь подчеркивает международный характер обмена данными, ведь вьетнамские приложения на смартфоне отсутствовали.

Несмотря на полное бездействие пользователя, продолжали потреблять данные, хотя большая часть трафика и пришлась на обновления приложений в Google Play и другие сервисы Google. Помимо этого, исследование выявило проблему чрезмерных разрешений, которые запрашивают приложения, большинство из которых не требуется для корректной работы приложения, но которые в ряде случаев не могут быть отозваны без полного удаления программного пакета.

securitylab.ru

Уязвимость системы позиционирования объекта для спуфинг-атак

УДК 004.056

Представленная работа посвящена исследованиям в области защиты навигационного канала, используемого для позиционирования объекта. В качестве исследуемого объекта использовался дрейфующий буй Черноморского гидрофизического подспутникового полигона с системой спутникового позиционирования. Обеспечение информационной безопасности в спутниковых сетях требует применения различных мер, таких как шифрование данных, аутентификация пользователей, контроль доступа, обучение персонала правилам безопасности и конфиденциальности, а также разработки стандартов и рекомендаций специализированными организациями.

Ключевые слова: спуфинг-атака, навигационный сигнал, позиционирование, защита информации, уязвимость объекта

Игорь Николаевич Карцан
kartsn2003@mail.ru
ФГБУН ФИЦ «Морской гидрофизический институт РАН»
ФГБОУ ВО «Сибирский государственный университет науки и технологий им. академика М. Ф. Решетнева»

En **Vulnerability of the Positioning System to Spoofing**

I. N. Kartsan
kartsn2003@mail.ru
Marine Hydrophysical Institute, Russian Academy of Sciences
Reshetnev Siberian State University of Science and Technology

The presented paper is devoted to research in the field of protection of navigation channel used for positioning of the object. The drifting buoy of the Black Sea hydrophysical sub-satellite polygon with a satellite positioning system was used as the object under study. Information security in satellite networks requires the use of various measures such as data encryption, user authentication, access control, training of personnel in security and privacy rules, as well as the development of standards and recommendations by specialized establishments.

Keywords: spoofing attack, navigation signal, positioning, information protection, object vulnerability

Введение

В современном информационном обществе спутниковые навигационные системы играют все большую роль в повседневной жизни людей и различных отраслях промышленности. Они обеспечивают надежную и точную навигацию, позволяют определить местоположение объектов с высокой степенью точности и предоставляют ценную информацию для всевозможных приложений [1–4].

Более того, с развитием технологий и доступности электронных средств связи, включая радио- и спутниковую связь, увеличивается риск несанкционированного доступа к персональным устройствам, использующим спутниковые навигационные системы, или их взлома. Хакеры могут злоупотребить слабыми местами в системе и получить доступ к личным данным, а также вмешаться в нормальную работу системы.

Однако вместе с быстрым развитием и использованием спутниковых навигационных систем возникает потребность в систематическом анализе уязвимостей и возможных рисков, связанных с каналами связи, используемыми в этих системах. С целью обеспечения безопасности передачи данных и их защиты от возможных атак необходимо провести тщательный анализ всех возможных слабых мест в каналах связи [6, 7].

Спуфинг-атаки представляют собой опасный вид кибератак, основанный на маскировке или подмене идентификационных данных, с целью обмана оператора связи и про-

никновения в защищенные системы или сети. Этот метод хакерства позволяет злоумышленникам создавать иллюзию подлинности, заставляя жертву доверять поддельным информационным источникам или взаимодействовать с поддельными учетными записями и сертификатами [5, 8–13].

Стратегия спуфинг-атак заключается в использовании различных методов манипуляции данными, чтобы убедить жертву в том, что они имеют дело с доверенным источником информации или с доступным для них сервисом. Некоторые наиболее распространенные спуфинг-техники включают подделку IP-адреса, фальшивые электронные письма (фишинг), создание поддельных web-сайтов, участие в сетевых атаках под другими именами и пр. [14–18].

После успешного выполнения спуфинг-атаки, злоумышленнику становится возможно выполнить различные виды мошенничества, отвлекая жертву от контроля над своими учетными записями и конфиденциальными данными. Возможные последствия включают кражу личной информации, финансовые мошенничества, вандализм или использование заразившегося устройства для продолжения атак на другие цели.

Постановка задачи

Одним из наиболее опасных злоумышленных воздействий в отношении систем спутникового позиционирования является возможность перехвата и подмены данных, передаваемых между спутниками и навигационной аппаратурой пользователя. Исследовательским объектом в ходе исследования использовался дрейфующий буй Черноморского гидрофизического подспутникового полигона с системой спутникового позиционирования навигационной системы ГЛОНАСС. Дрейфующий буй оснащен:

- навигационной аппаратурой пользователя (НАП) ГЛОНАСС, которая принимает сигналы с открытым доступом (значение центральной частоты: 1246 МГц и 1602 МГц);
- аппаратурой приема-передачи данных через систему спутниковой связи «Гонец» (для передачи: 312…315 МГц, для приема: 387…390 МГц);
- полезной нагрузкой дрифтера, включающей аппаратуру сбора информации из подводной среды.

Данная комплексная система позволяет оперативно собирать и передавать информацию об подводной обстановке с координатной привязкой. Одно из направлений исследования заключается в выявлении основных уязвимых мест при спуфинговых атаках на спутниковую систему навигации на морской поверхности, включая определение основных функций и методов атаки, а также в выборе направлений работы по минимизации влияния таких атак на позиционирование объекта. При минимизации влияния спуфинг-атак позиционирования на морские дрейфующие буи необходимо учитывать существующие ограничения (масса, габаритные размеры, энергопотребление и др.). Существующими ограничениями возможно частично пренебречь, но в данном варианте на первом месте будет стоять важность решаемой морским буем задачи.

Сценарий спуфинг-атаки на объект позиционирования

Воздействия на находящийся в одной координатной сетке объект осуществлялось с береговой линии с применением следующей аппаратуры: устройства для глушения спутникового сигнала, ВЧ-усилителя, направленной антенны и специального программного обеспечения (рис. 1).

Оказание влияния на объект, находящийся в одной координатной сетке (неподвижный), является высокотехнологичным и хорошо спланированным процессом, особенно если инициаторы атаки стремятся нейтрализовать объект с минимальными для себя потерями и максимальным ущербом для его функциональности.

Атака начинается с определения места и времени, где и когда объект окажется в наиболее благоприятных условиях для выполнения текущей задачи либо той, для которой он предназначен. Для этого инициаторы атаки могут использовать различные источники информации, включая открытые данные и анализ ситуации на местности.

Далее происходит проникновение в систему управления объектом, чтобы получить контроль над его функциями и системой маневрирования. Это может быть достигнуто с использованием различных технических методов, включая взлом радиосигналов, внедрение вредоносного программного обеспечения или физический доступ к объекту для установки устройств слежения или манипуляции с его системами.

Получив контроль над объектом, инициаторы атаки могут решить, как лучше всего использовать объект для собственных целей. Они способны заглушить передачу данных с объекта, чтобы затруднить его функционирование и дезориентировать его операторов. Кроме того, могут быть использованы специальные техники маскирования своего присутствия в системе во избежание преждевременного обнаружения. Также могут использоваться перехваченные данные с других схожих объектов и сенсорные данные для синхронизации своего подхода.

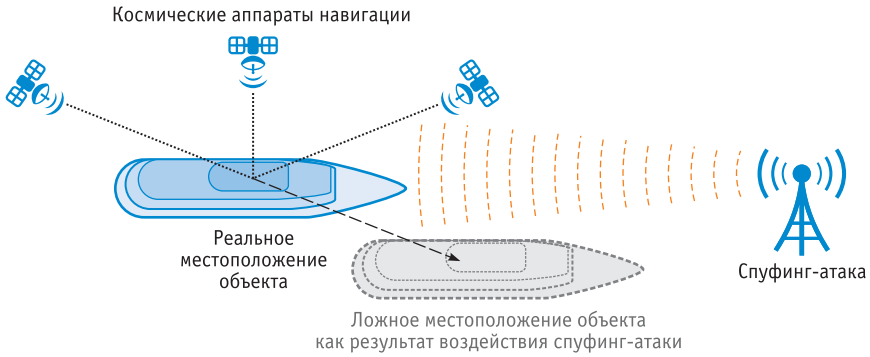


Рис. 1. ***Подмена навигационного сигнала более мощным с целью внесения ошибки позиционирования для неподвижного объекта***

Таким образом, атака на неподвижный объект требует высокой степени технической грамотности, планирования и координации действий. Однако, несмотря на повышенную сложность, с развитием кибертехнологий они становятся все более реальными и требуют к себе повышенного внимания.

В качестве примера атаки на движущийся объект рассмотрим случайную ситуацию, когда объект находится в движении по заранее заданной траектории (рис. 2). Целью атаки является уничтожение или нейтрализация объекта либо получение информации о стоящих перед ним задачах или применяемых в нем технологиях.

Для успешной атаки злоумышленник изучает траекторию движения объекта с применением радаров, определяет уязвимые места и моменты для атаки, также собирает информацию о бортовых системах объекта и любых слабых местах, которые можно использовать для атаки. Уязвимыми местами объекта могут выступать его двигатели, коммуникационные системы или навигационное оборудование.

Способы атаки на объект:

- физическое контактное воздействие для полного или частичного разрушения объекта;
- дистанционное воздействие с использованием радиоэлектронных систем для нарушения коммуникативных связей или блокировки систем управления, в том числе для изменения его траектории движения.

В обоих случаях цель атаки будет достигнута при нарушении функциональности: стоящие перед объектом задачи не смогут быть выполнены.

После моделирования каждой атаки проводился анализ предпринятых действий с целью определения эффективности использованных методов защиты и нападения и выявления причин, по которым атака была успешной либо неуспешной.

Подход к минимизации влияния спуфинг-атак на системы позиционирования объекта

Успешное противодействие спуфинг-атакам предполагает непрерывное развитие систем и методов их предотвращения, с одной стороны, и защиты объектов, использующих спутниковую систему позиционирования, с другой.

Исследование и анализ данных о количестве навигационных спутников используемых НАП при спуфинг-атаке позиционирования, становятся неотъемлемой частью работы экспертов и аналитиков в данной области. Результат представления таких данных является важным и информативным инструментом для понимания актуальной ситуации и прогнозирования возможных сценариев развития событий. На основе этого результата можно оценить уровень уязвимости и готовность национальной спутниковой системы к потенциальным атакам и сбоям.

Здесь необходимо учитывать использование спутников, предназначенных для выполнения различных функций, включая навигацию, связь, разведку и др. Получаемые ими данные представляют собой ценную информацию о состоянии и эффективности спутниковой системы, что позволяет анализировать ее работоспособность и улучшать ее производительность. Исследование и анализ данных, полученных в ходе моделирования атак, требует высокой экспертизы, технического мастерства и глубокого понимания функционирования навигационных спутниковых систем. Результаты этой работы поспособствуют принятию обоснованных решений в будущем и разработке эффективных стратегий обеспечения безопасности.

Приведем методы защиты от атак на позиционирование с использованием спутниковой навигации, которые требуют более детального исследования и оптимизирования. Первый из них – это применение антенн с управляющей диаграммой направленности по сигналу, что позволит не только отфильтровать шум и помеху в виде атаки, но и определять направление вредоносного сигнала. Таком образом, данный метод позволяет отличить ложный спутниковый сигнал от реального. Второй метод – применение вычислительной системы с алгоритмом сравнения сигналов до приемной навигационной аппаратуры, что позволит постоянно сравнивать навигационный сигнал с набором правил для выявления ложных схожих сигналов и дальнейшей их фильтрации. Третьим методом, способным существенно повысить надежность позиционирования объекта, является одновременное использование не менее двух систем навигации.

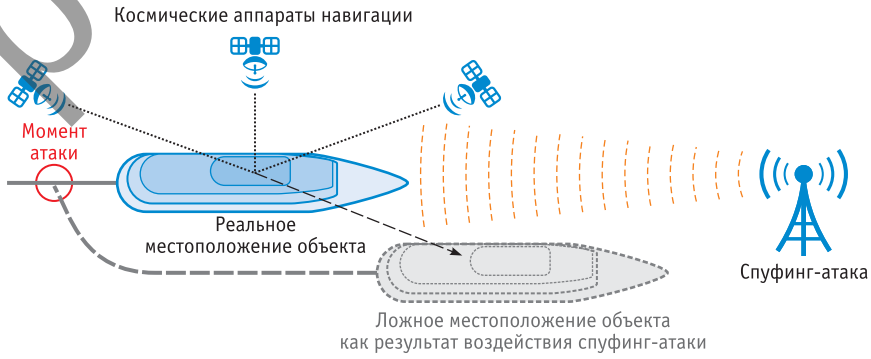


Рис. 2. ***Подмена навигационного сигнала более мощным с целью внесения ошибки позиционирования для подвижного объекта***

Выводы

Технологии, обеспечивающие защиту от спуфинг-атак позиционирования, только начинают развиваться, тем не менее, для крупных систем, таких как морская навигация судоходства, в настоящее время они уже созданы.

Для предотвращения спуфинг-атак и защиты от них требуется несколько мер безопасности. Во-первых, необходимо обучение пользователей навигационных устройств и сетей распознаванию подозрительных запросов, чтобы предостерегать их от взаимодействия с не-

доверенными источниками. Во-вторых, важно установить в НАП современные программные фильтры и системы обнаружения угроз, которые могут помочь идентифицировать спуфинг-атаки и блокировать их до причинения ущерба.

Борьба с проблемой спуфинг-атак требует постоянного совершенствования систем безопасности, а также внимательности и бдительности со стороны пользователей. Только путем осознания рисков и принятия соответствующих мер можно минимизировать угрозы и охранять информацию в мире, где спуфинг-атаки становятся все более распространенными и изощренными.

Вместе с тем, не стоит забывать, что существуют и другие потенциальные угрозы каналам связи, такие как возможность отказа в обслуживании (DoS-атаки), атаки на шифрование и аутентификацию, компрометация системных компонентов и т. д., соответственно, их предотвращение также требует проведения всестороннего анализа и разработки соответствующих контрмер и защитных механизмов. ■

Работа выполнена в рамках государственного задания по теме № FNNN-2024-0016.

ЛИТЕРАТУРА

1. *Карцан И. Н., Охоткин К. Г., Карцан Р. В., Пахоруков Д. Н. Эффективность радионавигационных систем // Вестник Сибирского гос. аэрокосмического ун-та им. академ. М. Ф. Решетнева. – 2013. – № 3 (49). – С. 48–50.*
2. *Аннилогов В. Н., Карцан И. Н. Основные области применения геоинформационных систем // Решетневские чтения. – 2011. – Т. 1. – С. 160–161.*
3. *Жукова Е. С., Литошик С. В., Колесник В. И., Карцан И. Н. Область применения космической навигации // Решетневские чтения. – 2010. – Т. 1. – С. 146–148.*
4. *Жуков А. О., Карцан И. Н., Аверьянов В. С. Кибербезопасность Арктической зоны // Информационные и телекоммуникационные технологии. – 2021. – № 51. – С. 9–13.*
5. *Басан Е. С., Абрамов Е. С., Басюк А. Г., Сушкин Н. А. Метод обнаружения атак на систему навигации БПЛА // Информатика и автоматизация. – 2021. – № 6 (20). – С. 1368–1394.*
6. *Аверьянов В. С., Карцан И. Н. Об атаке расщепления в распределении криптографических ключей безопасности // Защита информации. Инсайд. – 2022. – № 4 (106). – С. 20–23.*
7. *Eldosouky A., Ferdowsi A., Saad W. Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing // IEEE Internet of Things Journal. 2020. № 4 (7). P. 2840–2854.*
8. *Аверьянов В. С., Карцан И. Н. Безопасность ключевой последовательности по протоколу Чарльза Беннета // Сб. науч. статей по мат. Всерос. науч. конф. «Российская наука, инновации, образование – РОСНИО-2022». – Красноярск. – 2022. – С. 72–75.*
9. *Korotkevich A., Saad H. Kh., Stupin K. Models of GPS-spoofing of civil navigation equipment of consumers // Новости науки и технологий. – 2021. – № 4 (59). – С. 48–56.*
10. *Сосулин Ю. Г., Костров В. В., Паршин Ю. Н. Оценочно-корреляционная обработка сигналов и компенсация помех. – М.: Радиотехника – 2014. – 632 с.*
11. *Нуриев С. А., Карцан И. Н. Совершенствование цифровых каналов связи // Защита информации. Инсайд. – 2023. – № 5 (113). – С. 2–6.*
12. *Вексельман М. И. Безопасность систем синхронизации на основе гнсс. мониторинг качества навигационных систем // Радионавигация и время: труды СЗРЦ Концерна ВКО «Алмаз-Антей». – 2022. – № 10 (18). – С. 20–27.*
13. *Аксельрод В. А., Аверьянов В. С., Карцан И. Н. Протокол распределения квантовых ключей BB84 // Сб. науч. статей по мат. Всерос. науч. конф. «Российская наука, инновации, образование – РОСНИО-2022». – Красноярск. – 2022. – С. 142–147.*
14. *Карцан И. Н., Контылева Е. А. Глубокий интернет вещей // Современные инновации, системы и технологии. – 2023. – Т. 3, № 2. – С. 0201–0212. – DOI: 10.47813/2782-2818-2023-3-2-0201-0212.*
15. *Юкин И. В. Навигационное использование системы e-loran в модификации с методом сплайн-функций // Вестник государственного университета морского и речного флота им. адмирала С. О. Макарова. – 2020. – № 4 (12). – С. 703–715.*
16. *Максименко В. Н., Ухин Д. А. Анализ уязвимостей каналов связи спутниковых навигационных систем LBS-услуги // Экономика и качество систем связи. – 2019. – № 1 (11). – С. 18–22.*
17. *Мухортов В. В., Королев И. Д., Шкуринский С. В. Защита систем спутниковой навигации от внешних программно-аппаратных воздействий // Инновации в науке: сб. ст. по матер. LV междунар. науч.-практ. конф. – № 3 (52). Часть II. – Новосибирск: СибАК. – 2016. – С. 102–108.*
18. *Монзинго Р. А., Миллер Т. У. Адаптивные антенные решетки. – М.: Радио и связь. – 1986. – 448 с.*

Цифровая криминалистика распределенных реестров

Методическое пособие

Применение криптографии высокого уровня позволило создать практически безупречную репутацию для распределенных реестров в части надежности и скорости работы. Они все чаще применяются для ведения государственных реестров, создания баз данных со значимой информацией и пр.

Вместе с тем, идеальных технологий не существует, и хранение информации в распределенных реестрах также подвержено определенным рискам.

В настоящем учебно-методическом пособии приведены основополагающие принципы функционирования криптовалют, на практических примерах обозначены риски их использования, представлены некоторые особенности операций с криптовалютой. Кратко рассмотрена российская судебная практика в сфере виртуальных активов. Намечены перспективы развития рассматриваемой области. На примере сервиса российских разработчиков рассмотрена вероятность оценки совокупности признаков, идентифицирующих субъектов, возможных владельцев кошельков по принадлежности к биржам, миксерам и пр.

Пособие предназначено для широкого круга читателей, интересующихся данной тематикой.

Ознакомиться с подробным содержанием пособия и оформить заказ можно на сайте www.inside-zi.ru

О применении в криптологии квантового преобразования Фурье

УДК 004.77; 004.056.5

Квантовые вычисления – одно из приоритетных научно-технических направлений для достижения технологического суверенитета Российской Федерации. В основе квантовых вычислений лежат междисциплинарные исследования информатики, физики и математики на принципах квантовой механики для ускорения решения вычислительно сложных для классических компьютеров фон Неймана задач. Здесь особый интерес вызывает квантовый алгоритм Шора, который способен факторизовать целые числа за полиномиальное время, что ставит под угрозу стойкость традиционных криптографических систем RSA, DSA, EdDSA, ГОСТ Р 34.10-2012 и др., не обладающих свойством квантовой устойчивости. Однако на практике реализация алгоритма Шора сталкивается с рядом технических проблем, ключевой из которых является эффективное построение квантового преобразования Фурье (QFT) – важнейшей составляющей упомянутого алгоритма. В настоящей статье рассмотрен новый гибридный подход построения аппроксимированного квантового преобразованию Фурье (AQFT) с ограниченным числом вентилей, направленный на оптимизацию алгоритма Шора. Предлагается способ последовательного применения различных методов сокращения квантовых ресурсов и повышения эффективности схемы квантового преобразования Фурье, которые критичны для улучшения производительности алгоритма Шора с требуемой точностью при ограниченных ресурсах.

Ключевые слова: квантовая угроза, квантовое преобразование Фурье, квантовая устойчивость, квантовая и постквантовая криптография, стойкость криптопримитивов, квантово-устойчивые криптосистемы

Алексей Сергеевич Петренко
a.petrenko1999@rambler.ru
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Введение

Квантовое преобразование Фурье, являясь центральным элементом многих квантовых алгоритмов, требует солидных ресурсов и высокой точности реализации [10, 15]. Проблемы, связанные с числом вентилей и точностью AQFT, ограничивают масштабируемость и практическое применение алгоритма Шора [18, 19, 28, 30]. В ответ на эти вызовы рассмотрим гибридный подход к оптимизации AQFT, сочетающий методы аппроксимированного преобразования Фурье с техниками уменьшения числа вентилей. Он направлен на минимизацию квантовых ресурсов, необходимых для эффективной реализации алгоритма Шора, при одновременном сохранении достаточно высоких точности и устойчивости к ошибкам.

En **On the Application of the Quantum Fourier Transform in Cryptology**

A. S. Petrenko
a.petrenko1999@rambler.ru
Saint-Petersburg State Electrotechnical University «LETI»

Quantum computing is based on interdisciplinary research from computer science, physics and mathematics using the principles of quantum mechanics to speed up the solution of computationally complex problems compared to von Neumann computers. Here, of particular interest is Shor's quantum algorithm, which is capable of factoring integers in polynomial time, which threatens the strength of traditional cryptographic systems. However in practice, its implementation faces a number of technical problems, the key of which is the effective construction of the quantum Fourier transform (QFT). This article discusses a new hybrid approach to constructing an approximate quantum Fourier transform (AQFT) with a limited number of gates, aimed at optimizing the Shor algorithm. A method is proposed to sequentially apply various methods for reducing quantum resources and increasing the efficiency of the quantum Fourier transform circuit, which are critical for improving the performance of the Shor algorithm with the required accuracy under limited resources.

Keywords: quantum threat, quantum Fourier transform, quantum stability, quantum and post-quantum cryptography, strength of cryptoprimitives, quantum-resistant cryptosystems

Итак, для получения нужного результата потребовалось решить применительно к QFT (AQFT) две основные задачи: уменьшение вычислительной сложности и повышение точности. Для решения первой задачи рассмотрим QFT и AQFT в общем виде.

Оптимизация QFT достигается путем сокращения количества T-вентилей и выражается в сокращении T-счета. Как видно, исходное QFT нуждается в порядка $O(n^2)$ T-вентилях (операциях) для n кубитов (см. врезку п. 1).

Вместе с тем, в схемах AQFT вычислительная сложность уменьшена, минимум, до $O(n \log n)$ T-вентилей (операций) как за счет множественных модификаций, так и, главным образом, в результате ограничения углов вращения отдельных кубитов (см. врезку п. 2).

Таким образом, задача сводится к сокращению количества вентилей в построенных схемах, из которых T-вентили являются наиболее значимыми для вычислительной сложности, то есть к сокращению T-счета.

Известно, что для решения второй задачи – сокращения количества ошибок в квантовых вычислениях – зачастую используются алгоритмы коррекции ошибок. Однако в настоящей работе предлагается способ построения схем с частичной заменой T-вентилей на вентили CNOT, что позволяет достичь подобного эффекта без добавления отдельных алгоритмов со своей вычислительной сложностью. Данный способ основан на утверждении, что в среднем T-вентили могут быть в 10–10^4 раз более подвержены ошибкам, чем другие вентили (как однокубитные, так и более сложные). Это связано с тем, что для реализации T-вентиля часто требуется сложная последовательность операций, включая внутреннюю коррекцию ошибок и инъекцию так называемых магических состояний [2–17, 20–30].

Другими словами, данная задача сводится к наибольшему уменьшению числа T-вентилей в схемах таким образом, чтобы возникшая избыточность не создавала дополнительной вычислительной сложности из-за возникновения вентилей, предназначенных для построения, а не для функционирования новых схем на выбранных квантовых компьютерах.

Отметим, что данные задачи являются частично противоречивыми, поэтому в рамках гибридного подхода (в силу ограниченности современных квантовых мощностей) решение первой задачи выбрано приоритетным. Решение обеих задач позволяет существенно модифицировать криптоанализ с использованием квантового компьютера, а именно, посредством качественно новой модификации QFT (AQFT) в качестве самой вычислительно сложной составляющей алгоритма Шора (остальные шаги квантовой части алгоритма Шора – подготовка состояния суперпозиции и его построение – являются относительно простыми и практически не модифицируемыми).

Возможность реализации аппроксимированного QFT (AQFT) путем исключения элементов вращения с малыми углами открывает новые перспективы в эффективности и точности квантовых алгоритмов. Пример такой схемы AQFT представлен на рис. 1. Более ранние практические исследования показали, что подобная схема AQFT с примерно $5{,}3 \times 10^4$ управляемыми вентилями вращения может эффективно факторизовать 1024-битные числа с предполагаемой точностью более 99,9 %. Такая аппроксимация уже широко изучена, и ее надежность на квантовых компьютерах подтверждена серией экспериментов [1, 7, 9].

В то же время, оптимизация AQFT с ограничением числа вентилей может привести к повышению эффективности квантовых алгоритмов. В рамках исследования предлагается новый алгоритм для создания схем AQFT в архитектуре ближайшего соседа, используя вентили CNOT вместо SWAP, что уменьшает количество вентилей и упрощает схему.

Данный подход апробирован в вычислительной среде IBMQ наряду с традиционными схемами AQFT,

Врезка

1) $\mathrm{QFT}|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{N}} |y\rangle,$

где $|x\rangle$ – входное квантовое состояние;

$N = 2^n$ – общее количество состояний;

$|y\rangle$ – базисные состояния, по которым происходит суммирование;

$e^{\frac{2\pi i x y}{N}}$ – фазовый фактор, влияющий на амплитуду каждого базисного состояния в сумме.

2) $\mathrm{AQFT}|x\rangle \mapsto \frac{1}{\sqrt{N}} \cdot \sum_{y=0}^{N-1} \left(\prod_{k=1}^{n} e^{\frac{2\pi i x y}{N} \cdot f(k,p)} \right) |y\rangle,$

где $f(k, p)$ – некоторая функция, определяющая, какие взаимодействия между кубитами учитываются, а какие нет, в зависимости от их расстояния k и уровня приближения p.

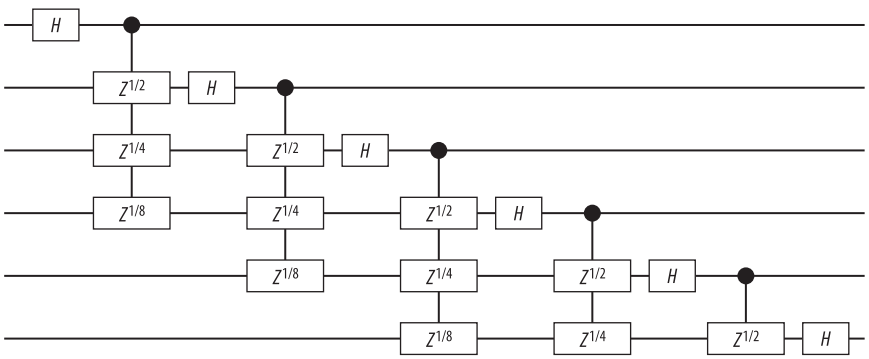


Рис. 1. ***Пример AQFT с параметрами n = 6 и b = 3***

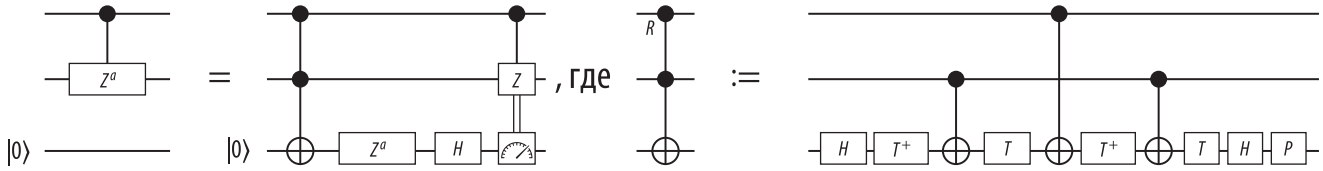


Рис. 2. ***Вспомогательная оптимизация вентиля Z^a с помощью добавления измерения на основе прямой связи для повышения отказоустойчивости***

в результате чего было подтверждено, что полученные схемы обладают практически значимым выигрышем как в ресурсоемкости, так и в эффективности архитектуры ближайшего соседа квантовых компьютеров IBMQ. Предполагается, что гибридный подход построения оптимизированного AQFT может эффективно использоваться в различных квантовых алгоритмах, в частности, в алгоритме Шора, существенно повышая их эффективность в ограниченных квантовых вычислительных средах.

Предлагаемый подход

Вследствие чрезвычайной чувствительности квантовой информации к разного рода ошибкам, для реализации сложных алгоритмов, наподобие алгоритма Шора, с целью исправления ошибок необходимо применять отказоустойчивые вычисления, которые включают использование нескольких физических кубитов для представления одного логического кубита. Эффективные отказоустойчивые схемы должны минимизировать использование T-вентилей и подобных им, поскольку они значительно более ресурсоемки, чем вентили Клиффорда [2, 6, 12, 16, 31].

T-вентиль (или π/8-вентиль) является одним из важнейших квантовых вентилей, особенно в контексте квантовой логики, так как его сложно реализовать без ошибок. С помощью T-счета (количества T-вентилей) в квантовых вычислениях оценивается сложность квантовой схемы или алгоритма. Такое исчисление особенно актуально в области квантовой коррекции ошибок и отказоустойчивых квантовых вычислений, поэтому будет использоваться в данном исследовании вместо традиционных оценок из теории сложности.

Стандартный подход к реализации n-кубитного AQFT с заданной точностью и отказоустойчивостью включает аппроксимацию путем удаления малых углов управляемого вращения. Это позволяет сократить количество элементов с $O(n^2)$ до значений менее $O(n\log n)$. Здесь важно отметить, что нами будет рассмотрено только полностью когерентное AQFT, в отличие от вариантов, где после AQFT происходит измерение. В настоящем исследовании используется оптимизированное AQFT с целью уменьшения T-счета до менее чем $O(n\log n)$. Этот подход обеспечивает баланс между точностью и аппроксимацией, сохраняя высокую точность вычислений даже при уменьшенном количестве вентилей.

При рассмотрении стоимости квантовой схемы также следует учитывать различные типы связи между кубитами, так как физические ограничения квантового оборудования чаще всего приводят к тому, что квантовые схемы двухкубитных вентилей будут находиться в архитектуре ближайшего соседа (архитектура ближайшего соседа предполагает, что кубит в схеме взаимодействует только с соседними кубитами). Преимущество же преобразования, при котором схема AQFT использует вентили CNOT вместо вентилей SWAP, заключается в том, что в первом случае она будет более компактной, поскольку для замены каждого вентиля SWAP требуется три значительно более вычислительно простых вентиля CNOT. После переупорядочения кубитов гейтовая (вентильная) схема AQFT с n-кубитами и ближайшими соседями требует всего n^2+n-4 вентилей CNOT.

Основой для создания оптимизированной схемы AQFT является стандартная реализация схемы AQFT с использованием параметризованных $O(n^2)$ вращений с контролируемым Z^a, где $a\in\{1/2, 1/4, \ldots, 1^{n-1}/2\}$ и n вентилей Адамара, представленная на рис. 2. AQFT можно получить из схемы, отбросив вращения с параметром a ниже определенного порога, сохранив только b контролируемых вращений на слой, при этом параметр b масштабируется логарифмически с n.

Стандартная отказоустойчивая реализация AQFT с приблизительно $n\log(n)$ параметрически определенными управляемыми вращениями определяет, в свою очередь, $b=\log(n)$ для простоты схемы и независимости от ошибок аппроксимации. При этом в такой схеме используется приблизительно $12n\log^2(n)$ T-вентилей, поскольку 4 T-вентиля используются для отображения управляемых вращений в неконтролируемые и приблизительно $3\log(n)$ T-вентилей необходимы для аппроксимации неконтролируемых вращений.

Указанную схему можно дополнительно оптимизировать, если учесть, что неконтролируемые вращения происходят слоями и, таким образом, могут быть вызваны с помощью вентиля-сумматора, имеющего доступ к $\log(n)$-кубитному градиентному состоянию.

На рис. 3 изображена такая схема после применения сумматоров к общим фазовым сдвигам, где вентиль ψ обозначает подготовку специального состояния $|\psi_{b+1}\rangle$. При этом U_i иллюстрирует операции, предшествующие i-му сумматору, включающие H-вентили и фазовые вен-

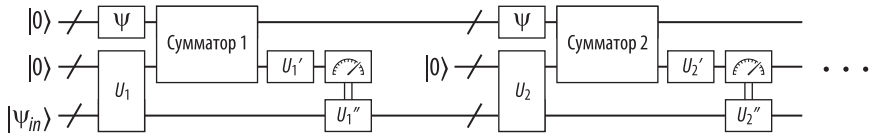


Рис. 3. ***Схема общего вида реализации отказоустойчивости в гибридном AQFT***

тили Тоффоли, используемые для преобразования управляемых Z_a-вращений в неуправляемые Z_a-вращения. U_i обозначает операции, которые следуют за сумматором вплоть до внутрисхемных измерений, а U_i'' – управляемые вентили Z, применяемые на i-м шаге.

Использование эффективного b-битного целочисленного сложения r с примерно $4b$ T-вентилями позволяет снизить требования к T-вентилям в схеме с приблизительно $12n\log^2(n)$ до приблизительно $8n\log(n) + 3\log^2(n)$, где 4 T-вентиля применяются для передачи управления, еще 4 T-вентиля необходимы для целочисленного сложения на каждое контролируемое вращение, а $3\log(n)$ T-вентиля используются на каждом из $\log(n)$-кубитов для синтеза $\log(n)$-кубитного градиентного состояния, которое затем используется повторно. Такое сокращение вычислительной сложности дает существенное улучшение как в асимптотическом анализе, так и при подсчете вентилей [8, 11, 14, 24, 29].

Для дальнейшей гибридной оптимизации AQFT потребуется построить схемы с линейной архитектурой ближайшего соседа, используя тождества схем (рис. 5). Сначала мы делим стандартную схему AQFT, например, как показано на рис. 4, на множество подсхем наподобие изображенной на рис. 6*а*. После чего преобразуем указанные подсхемы с помощью разработанного для этого алгоритма в схемы с линейной архитектурой ближайшего соседа, производим ряд оптимизаций и объединяем их, что будет показано далее.

Данный алгоритм применим ко всем составляющим схемы AQFT и в рассмотренном примере заключается в оптимизации схемы, изображенной на рис. 6*а*:

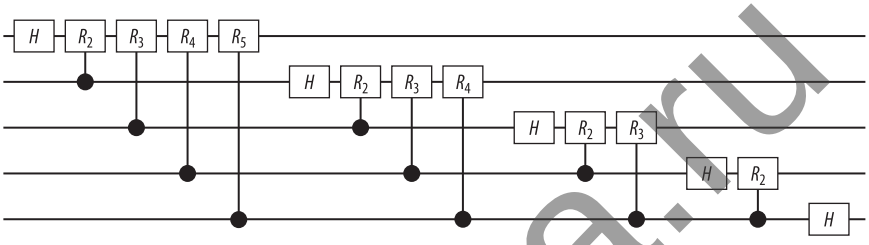


Рис. 4. ***Стандартная схема оптимизированного AQFT до применения сумматоров***

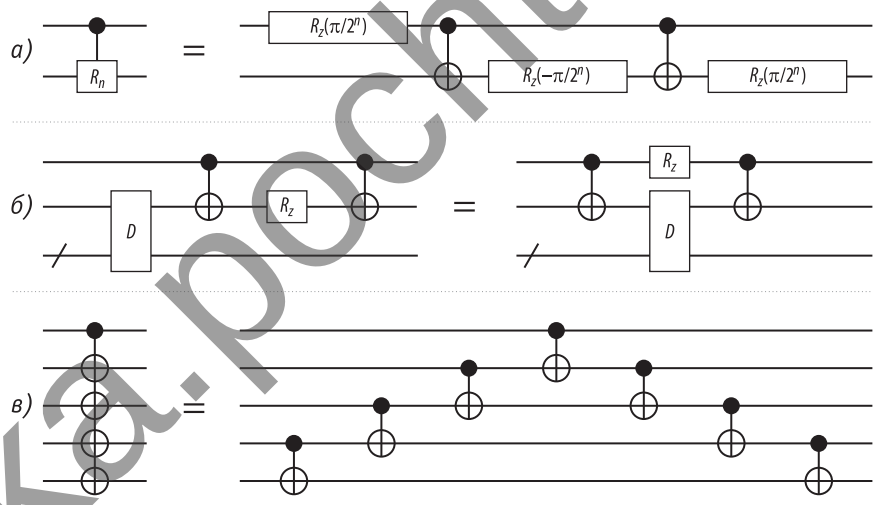


Рис. 5. ***Тождества, используемые в алгоритме***

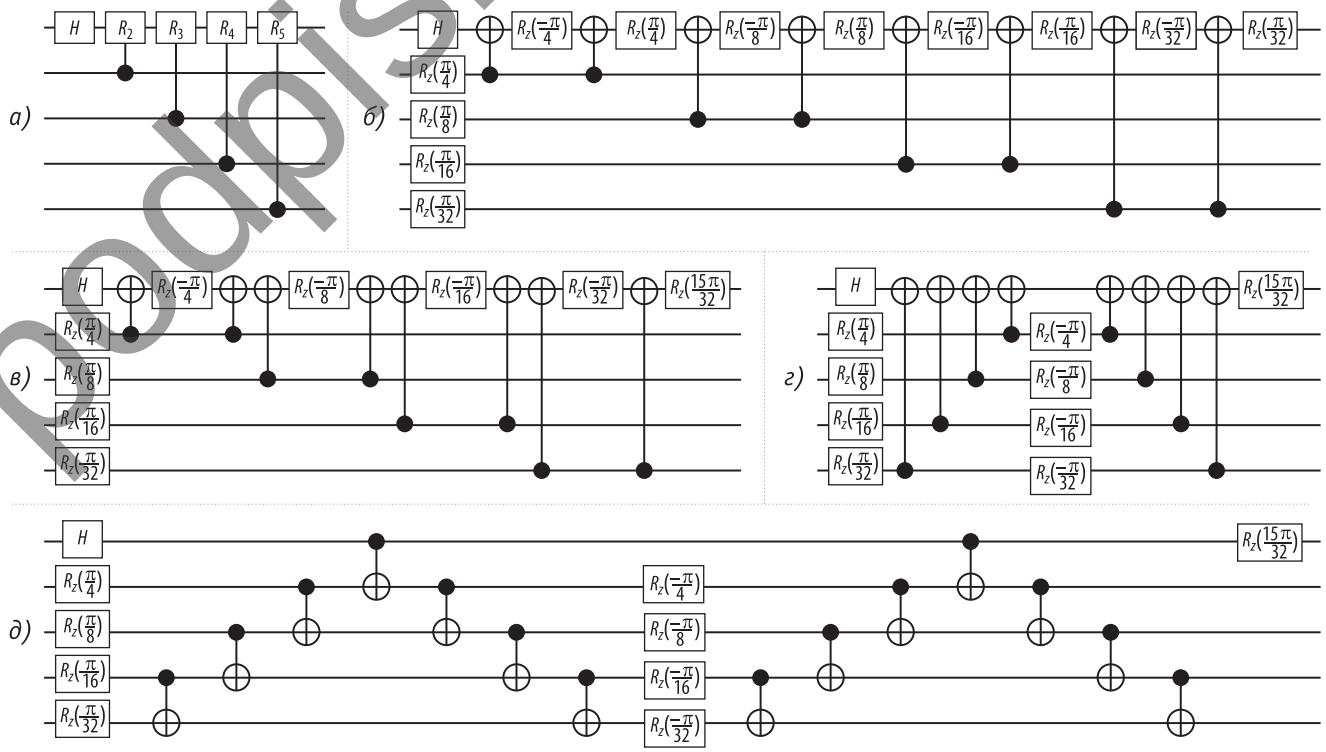


Рис. 6. ***Преобразования оптимизированного AQFT по ходу алгоритма***

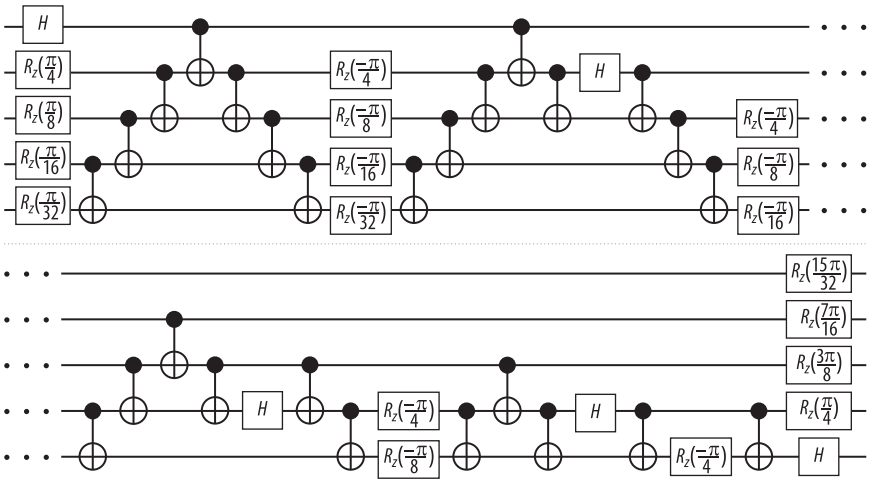


Рис. 7. ***Пример оптимизированного AQFT при n = 5 после объединения подсхем***

1) применить тождество схем на рис. 5*а* к схеме на рис. 6*а*, в результате чего схема на рис. 6*а* преобразуется в схему на рис. 6*б*;

2) объединить несколько вентилей R_Z, основываясь на утверждении, что схемы с диагональными матричными представлениями коммутируют друг с другом, в результате чего схема на рис. 6*б* преобразуется в схему на рис. 6*в*;

3) многократно применить тождество схем на рис. 5*б*, в результате чего схема на рис. 6*в* преобразуется в схему на рис. 6*г*;

4) применить тождество схем на рис. 5*в* к схеме на рис. 6*г*, в результате чего подсхема преобразуется в схему с архитектурой ближайшего соседа, представленную на рис. 6*д*.

Чтобы построить схему AQFT, необходимо применить описанный выше алгоритм ко всем подсхемам, объединить их и удалить соседние вентили CNOT. Следует отметить, что эта схема AQFT, представленная на рис. 7, также имеет линейную архитектуру ближайшего соседа. Таким образом, в общем случае становится возможным построить n-кубитную оптимизированную схему AQFT с архитектурой ближайшего соседа и приблизительно $n^2 + n - 4$ вентилями CNOT.

При апробации гибридной оптимизированной схемы AQFT была выбрана допустимая погрешность аппроксимации в 5–10 вентилей. Однако проведенный в ходе исследования анализ позволяет утверждать, что вероятностные ошибки аппроксимации незначительны и полностью компенсируются остальными оптимизационным решениями, не влияя на заявленную вычислительную сложность в виде T-счета.

Для случая n-кубитов реализованная схема AQFT, при сравнении с предыдущими аналогичными исследованиями, уменьшает количество вентилей CNOT, как минимум, на 16 %. Результаты и сравнение вычислительных сложностей представлены в таблице.

Заключение

В рамках исследования был представлен новый гибридный подход к построению оптимизированного аппроксимированного квантового преобразования Фурье (AQFT) с ограниченным числом вентилей, а также продемонстрировано, что этот подход значительно повышает эффективность алгоритма Шора, снижая общее количество необходимых вентилей и увеличивая точность вычислений.

Разработанная гибридная модификация AQFT была реализована на квантовых компьютерах IBMQ, так как они по умолчанию наследуют архитектуру более ранних квантовых компьютеров:

1) ibm_cairo, 27-кубитный квантовый компьютер с процессором Falcon r5.11;

2) ibm_sherbrooke, 127-кубитный квантовый компьютер с процессором Eagle r3;

3) ibm_torino, 133-кубитный квантовый компьютер с процессором Heron r1.

Таблица. ***Результаты апробации разработанного гибридного подхода и его сравнение с наиболее эффективным подходом к аналогичным модификациям***

Количество логических кубитов в построенной схеме AQFT	Схемы AQFT, разработанные с помощью гибридного подхода			Наиболее вычислительно простые схемы AQFT из числа «классических»			Приблизительный выигрыш в вычислительной сложности по T-счету, %
	Необходимое для выполнения схемы количество физических кубитов	Количество вентилей CNOT	T-счет	Необходимое для выполнения схемы количество кубитов	Количество вентилей CNOT	T-счет	
8	27	338	254	25	390	303	16,2 %
16	55	1496	968	51	1798	1162	16,8 %
32	79	3826	2218	67	4654	2698	17,8 %
64	113	8418	4686	99	10 366	5770	18,8 %
128	179	17 564	9604	163	21 790	11914	19,2 %
256	317	35 824	19 410	291	44 628	24 202	19,8 %
512	577	71 186	38 438	547	90 334	48 778	21,2 %
1024	1093	142 110	76 582	1059	181 726	97 930	21,8 %
2048	2115	284 336	153 064	2083	364 510	196 234	22,0 %
4096	4167	566 746	304 846	4131	730 078	392 842	22,4 %

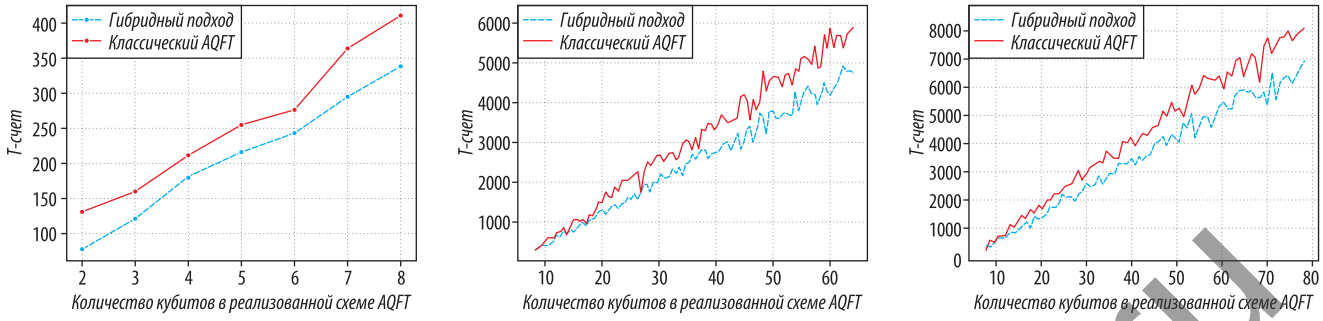


Рис. 8. ***Результаты построения AQFT с помощью гибридного подхода и «классическим» способом на квантовых компьютерах IBMQ согласно указанному порядку***

Каждая схема AQFT в ходе эксперимента транслировалась на квантовый компьютер 100 раз. Результаты эксперимента, представленные на рис. 8, позволили получить минимальные количества вентилей, необходимые для синтеза AQFT в каждом случае, которые оказались существенно меньше аналогичных показателей как классического QFT, так и его наиболее выигрышных модификаций в виде различных схем AQFT.

С одной стороны, при исследовании влияния размера решетки на качество векторов, полученных после гибридной оптимизации AQFT, было обнаружено, что преимущества оптимизационных методов становятся более значительными с увеличением размерности решетки. С другой стороны, рассмотрение использования независимых квантовых процедур для снижения общего размера квантовой схемы позволило достичь более эффективной факторизации чисел.

Была проведена серия экспериментов по построению AQFT с помощью разработанного гибридного подхода и в «классическом» виде. Обе поставленные в рамках исследования задачи выполнены, несмотря на существенные расхождения прогнозируемых в теории значений T-счета с полученными на практике значениями. Таковые объясняются ошибками декогеренции, а также несовершенством схем квантовых процессоров. Однако выявленные расхождения никак не влияют на полученный результат и оценку выигрыша в вычислительной сложности и точности полученных схем.

Кроме того, результаты, достигнутые в результате апробации на квантовых компьютерах ibm_sherbrooke и ibm_torino, позволяют сформулировать гипотезу о качественном уменьшении вычислительной сложности построенных схем, несмотря на то что определить точную функцию в силу особенностей архитектуры современных квантовых компьютеров на текущий момент не представляется возможным.

Разработанный гибридный подход к построению схем оптимизированного AQFT может быть особенно полезен при будущих исследованиях с использованием AQFT с большим количеством кубитов. Он может быть реализован в схемах различной размерности, что открывает новые перспективы для модификации квантовых вычислений в виде не только алгоритма Шора, но и других квантовых алгоритмов. Как следствие, это предлагает новые пути решения сложных вычислительных задач в эпоху шумных квантовых вычислений промежуточного масштаба (NISQ) [21, 25, 27, 32]. ■

Статья подготовлена при поддержке «Гранта ИБ МТУСИ» № 19/23-К «Метод (технология) обеспечения квантовой устойчивости блокчейн-экосистем и платформ Цифровой экономики Российской Федерации»

ЛИТЕРАТУРА

1. Shor P. W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Proc. 35th Annual Symposium on Foundations of Computer Science. IEEE, 1994.

2. Nielsen M. A., Chuang I. L. Quantum Computation and Quantum Information // Cambridge University Press, 2000 [Электронный ресурс]. – URL: cambridge.org/9781107002173/ (дата обращения: 10.12.2023).

3. Banaszczyk W. New bounds in some transference theorems in the geometry of numbers // Mathematische Annalen. 1993. V. 296, № 4. P. 625–635.

4. Coppersmith D. An approximate Fourier transform useful in quantum factoring // Cornell University. 2002 [Электронный ресурс]. – URL: quant-ph/0201067/ (дата обращения: 10.12.2023).

5. Crandall R., Pomerance C. Prime numbers. A computational perspective // NY: Springer, second edition. 2005.

6. Cleve R., Watrous J. Fast parallel circuits for the quantum Fourier transform // In 41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000), IEEE Comput. Soc. Press, Los Alamitos, CA. 2000. P. 526–536.

7. Ekerå M., Håstad J. Quantum algorithms for computing short discrete logarithms and factoring RSA integers // In Post-quantum cryptography: Springer, Cham, 2017. V. 10346 of Lecture Notes in Comput. Sci. P. 347–363.

8. Gidney C., Ekerå M. How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits // Quantum. 2021. № 5. P. 433.

9. Gama N., Phong Q. N. Finding short lattice vectors within Mordell's inequality // In STOC'08, NY: ACM. 2008. P. 207–216.

10. Grover L., Rudolph T. Creating superpositions that correspond to efficiently integrable probability distributions. 2002 [Электронный ресурс]. – URL: arXiv:quant-ph/0208112/ (дата обращения: 12.12.2023).

11. Harvey D., van der Hoeven J. Integer multiplication in time O(n log n) // Ann. of Math. 2021. V. 193, № 2. P. 563–617.

12. Pomerance C. The expected number of random elements to generate a finite abelian group // Period. Math. Hungar. 2001. V. 43, № 1–2. P. 191–198.

13. Regev O. On lattices, learning with errors, random linear codes, and cryptography // J. ACM. 2009. V. 56, № 6. Art. 34, 40.

14. Seifert J.-P. Using fewer qubits in Shor's factorization algorithm via simultaneous Diophantine approximation // In Topics in cryptology – CT-RSA 2001 (San Francisco, CA). Springer, Berlin. 2001. V. 2020 of Lecture Notes in Comput. Sci. P. 319–327.

15. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM Rev. 1999. V. 41, № 2. P. 303–332.
16. Kitaev A. Y. Quantum Measurements and the Abelian Stabilizer Problem // arXiv preprint, 1995 [Электронный ресурс]. – URL: quant-ph/9511026/ (дата обращения: 10.12.2023).
17. Fowler A. G. et al. Surface codes: Towards practical large-scale quantum computation // Physical Review A. 2012. V. 86, № 3. P. 032324–032372.
18. Gottesman D. The Heisenberg Representation of Quantum Computers // arXiv preprint, 1998 [Электронный ресурс]. – URL: quant-ph/9807006/ (дата обращения: 10.12.2023).
19. Harrow A. W., Hassidim A., Lloyd S. Quantum Algorithm for Linear Systems of Equations // Physical Review Letters. 2009. V. 103, № 15. P. 1–24.
20. Grover L. K. Quantum Mechanics Helps in Searching for a Needle in a Haystack // Physical Review Letters. 1997. V. 79, № 2, P. 325–328.
21. Steane A. M. Error Correcting Codes in Quantum Theory // Physical Review Letters. 1996. V. 77, № 5. P. 793–797.
22. Abrams D. S., Lloyd S. Quantum Algorithm Providing Exponential Speed Increase for Finding Eigenvalues and Eigenvectors // Physical Review Letters [Электронный ресурс]. – URL: 1999 arxiv-quant-ph9807070/ (дата обращения: 12.12.2023).
23. Childs A. M., et al. Exponential Algorithmic Speedup by a Quantum Walk // Proc. of the thirty-fifth annual ACM symposium on Theory of computing, 2003.
24. Петренко А. Квантово-устойчивый блокчейн: научная монография. – СПб.: Питер. – 2023. – 384 с.
25. Petrenko A. Applied Quantum Cryptanalysis (научная монография «Прикладной квантовый криптоанализ») // River Publishers. 2023. – 256 p.
26. Петренко А. Квантовая угроза технологии блокчейн: учеб.-метод. пособие. – СПб: Изд. Дом «Афина». – 2022. – 105 с. [Электронный ресурс]. – URL: https://elibrary.ru/item.asp?id=50043242/ (дата обращения: 17.12.2023).
27. Петренко А. Параметрический выбор криптопримитивов для блокчейн-платформ: учеб.-метод. пособие – СПб: Изд. Дом «Афина». – 2022. – 100 с. [Электронный ресурс]. – URL: https://elibrary.ru/item.asp?id=50043211/ (дата обращения: 17.12.2023).
28. Петренко А. С., Петренко С. А., Бучнев А. А. Инновационная платформа для квантового криптоанализа известных криптопримитивов блокчейна // Защита информации. Инсайд. – 2023. – № 2 (110). – С. 58–67.
29. Петренко А. С., Петренко С. А. Метод оценивания квантовой устойчивости блокчейн-платформ // Вопросы кибербезопасности. – 2022. – № 3 (49). – С. 2–22.
30. Петренко А. С., Петренко С. А. Basic Algorithms Quantum Cryptanalysis (Основные алгоритмы квантового криптоанализа) // Вопросы кибербезопасности. – 2023. – № 1 (53). – С. 100–115.
31. Petrenko A. S., Petrenko S. A., Taran V. N. Universal quantum gate as a tool for modeling quantum cryptanalysis algorithms on a quantum circuit // CEUR Workshop Proceedings. Сер. AISMA 2021. 2022. P. 143–150.
32. Боев С. Ф., Петренко А. С., Петренко С. А., Ступин Д. Д. Квантовый криптоанализ криптосхем блокчейн-платформ // Многопроцессорные вычислительные и управляющие системы (МВУС-2022): сб. мат. Всерос. науч.-техн. конф. (Таганрог, 27–30 июня 2022 г.); [отв. ред. академик И. А. Каляев]. – Южный фед. ун-т. – Ростов-на-Дону; Таганрог: Изд-во Южного фед. ун-та. – 2022. – С. 12–20.

НОВОСТИ

Cyber Stage – первая комплексная программа поддержки российских ИБ-стартапов

ГК «Солар», архитектор комплексной кибербезопасности, при участии крупных отраслевых экспертов рынка представила первую в России комплексную программу поддержки предпринимателей в области ИБ и смежных направлений.

По результатам опроса ГК «Солар» 84 компаний сегментов B2E, B2B, B2G, сейчас со стартапами работает только 13 %. Одной из главных проблем, препятствующих более активному взаимодействию бизнеса со стартапами, является расхождение ожиданий и реальности.

В России на начало 2024 года зарегистрировано 230 ИБ-бизнесов. Это менее 2,3 % от всего количества ИБ-проектов в мире (9874), а например, в Израиле 469 ИБ-компаний при уровне ВВП вчетверо ниже российского. Этому способствует существенная доля госзаказа в общем объеме рынка ИБ, высокий экспортный потенциал ИБ-решений и благоприятная для развития стартапов среда.

Решить задачу улучшения среды и условий развития ИБ-стартапов в России эксперты рынка намерены в рамках программы Cyber Stage, которая охватывает широкий спектр задач от создания удобной платформы взаимодействия участников рынка ИБ и смежных направлений до стимулирования запуска принципиально новых проектов в пустующих или недостаточно обеспеченных продуктами и сервисами нишах ИБ.

Бизнес готов начинать работу со стартапом, как правило, на продвинутой или финальной стадии разработки, в то время как без внешней помощи начинающий проект не способен до нее «добежать». В сегодняшних условиях потребуется несколько десятков лет, чтобы прийти к количеству ИБ-компаний, характерному для стран-лидеров в этой отрасли. Создатели программы рассчитывают уже в ближайшие два года показать видимые результаты. Так, до конца 2025 года они рассчитывают привлечь не менее 1,5 млрд руб. финансирования и вывести на рынок до 10 новых продуктов.

Минимальные требования к участникам: компания должна иметь основную команду, продукт, направленный на решение задач или на улучшение комплексных сервисов и продуктов в сфере ИБ, и находиться на стадии прототипа и выше. По итогам оценки стартап получает рекомендации и предложения по тому или иному направлению сотрудничества.

Источник: пресс-служба «Солар»

Простой критерий оценки качества белого шума Ципфа – Мандельброта с линейной вычислительной сложностью

УДК 519.24; 53; 57.017

Клод Шеннон в середине прошлого века переложил оценку непрерывной энтропии термодинамики (температуры) на оценку энтропии текстов (дискретных последовательностей). Это сегодня стало классикой. К сожалению, для длинных чисел, например, кодов длинного ключа, оценка энтропии по Шеннону требует тестовых выборок огромного размера. Причина – экспоненциальная вычислительная сложность оценок энтропии по Шеннону. Одним из путей обхода экспоненциальной вычислительной сложности является переход к использованию энтропии Ципфа или в более общем виде энтропии случайных последовательностей языков Мандельброта. Как критерий Ципфа, так и критерий Бенуа Мандельброта, имеют линейную вычислительную сложность и могут быть использованы при оценке качества случайных последовательностей.

Ключевые слова: энтропия Шеннона, экспоненциальная вычислительная сложность, энтропия Ципфа, линейная вычислительная сложность, малые выборки, оценка качества белого шума

Александр Иванович Иванов,
доктор технических наук, профессор
ivan@pniei.penza.ru
АО «Пензенский научно-исследовательский электротехнический институт»

En A simple criterion for assessing the quality of Zipf – Mandelbrot White Noise with Linear Computational Complexity

A. I. Ivanov,
PhD (Eng., Grand Doctor), Full Professor
ivan@pniei.penza.ru
Penza Research Electrotechnical Institute

In the middle of the last century, Claude Shannon shifted the assessment of the continuous entropy of thermodynamics (temperature) to the assessment of the entropy of texts (discrete sequences). This has become a classic today. Unfortunately, for long numbers, such as long key codes, Shannon entropy estimation requires huge test samples. The reason is the exponential computational complexity of Shannon entropy estimates.

One way around exponential computational complexity is to use the Zipf entropy or, more generally, the entropy of random sequences of Mandelbrot languages. Both the Zipf criterion and the Benoit Mandelbrot criterion have linear computational complexity and can be used in assessing the quality of random sequences.

Keywords: Shannon entropy, exponential computational complexity, Zipf entropy, linear computational complexity, small samples, white noise quality assessment

Энтропия Шеннона (1951 год) и энтропия Ципфа (1949 год)

При использовании алгоритма оценки энтропии Шеннона требуются значительные вычислительные ресурсы. Причина этого состоит в том, что при длине ключа шифрования 256 бит шифртекст выглядит как случайная последовательность данных. Из-за экспоненциальной вычислительной сложности алгоритма Шеннона для достаточно надежной оценки энтропии требуется использование большой выборки анализируемых данных.

Формула Шеннона для протяженных последовательностей является очень длинной логарифмической сверткой (врезка 1).

Для протяженных последовательностей приходится ждать появления множества маловероятных событий. Именно это и порождает вычислительные трудности. Ради исторической справедливости отметим, что работе Шеннона [1] предшествовала не менее значимая работа Ципфа [2]. Последний взял собственную работу на английском и построил для нее словарик, при этом вместо обычной сортировки слов по начальным буквам и их сочетаниям, им была ис-

Врезка 1

$$H("x_1, x_2, \ldots, x_{256}") = -\sum_{i=1}^{2^{256}} P_i \cdot \log_2(P_i), \quad (1)$$

где P_i – малая вероятность появления i-го сочетания символов в тексте длиной 256 бит.

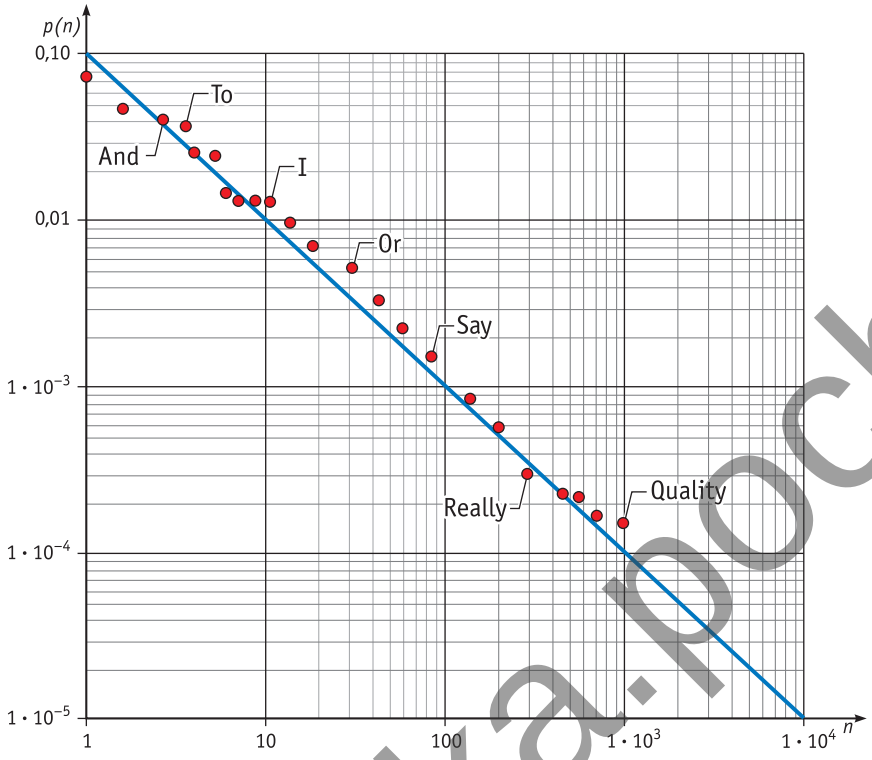


Рис. 1. ***Гиперболический закон Ципфа для текстов на английском***

пользована частота появления каждого слова в тексте. На рис. 1 представлена последовательность разных слов его словаря.

По словарю Ципфа мы имеем заранее вычисленные вероятности появления тех или иных слов в текстах на английском. Принципиально важной стороной подхода Ципфа является то, что оценка энтропии английского языка оказывается задачей линейной вычислительной сложности. В формуле (1) вместо вероятности появления сочетаний букв появилась вероятность появления слов, заранее вычисленная и размещенная в словаре. Словари всех реальных языков конечны, задача оценки энтропии кардинально упрощается. Как результат, энтропию Ципфа можно оценивать по фрагментам текста любой длины.

Задача быстрой и корректной оценки энтропии осмысленных текстов представляет существенный практический интерес для систем парольной защиты информации. Люди не могут запоминать длинные пароли из случайных символов, однако положение меняется, если человек запоминает фрагменты осмысленных текстов. При этом оценить энтропию длинных осмысленных паролей по Шеннону трудно из-за экспоненциальной вычислительной сложности задачи. Оценить энтропию по Ципфу несложно ввиду линейной вычислительной сложности этой задачи. Упрощение задачи обусловлено тем, что мы опираемся на готовые, заранее построенные таблицы вероятности появления слов на том или ином естественном языке пользователя. Если пользователь является носителем английского языка, то энтропию следует оценивать по данным рис. 1. Если пользователь говорит на другом естественном языке, то заранее должен быть построен иной словарь частот.

Энтропия случайных языков Мандельброта (1961 год)

Важным шагом в теории снижения вычислительной сложности оценки энтропии являются работы Бенуа Мандельброта [3–5], воспользовавшегося генератором псевдослучайных последовательностей. Повторяя ход рассуждений классика, будем считать, что случайный язык Мандельброта близок к русскому языку. Он имеет 31 букву и знак пробела между словами. Иные знаки препинания и заглавные буквы в новом случайном языке отсутствуют (устранены). Тогда кодировка каждого знака на этом случайном языке должна выполняться пятью битами.

Будем считать, что код пробела «0» для конкретного варианта языка дают три состояния кодов «0», «15», «31» в 32-арной системе счисления. В этом случае пробел будет появляться с вероятностью 3/32 (в три раза чаще иных значений случайного кода). Кроме того, будем считать, что парольная фраза на случайном языке будет состоять из текста длинной 55 знаков или иметь 255 бит бинарного кода (при анализе кодов длинной 256 бит нужно отбрасывать первый или последний бит).

Такой вариант пароля из 55 случайных букв воспроизводит программа на языке MathCAD, приведенная в верхней части рис. 2. Как и в случае анализа статистик Ципфа, статистики Мандельброта строятся на выделении длины слов (кодов между двумя пробелами).

Следует отметить, что все статистики случайных языков Мандельброта не имеют идеально гиперболического распределения. Они являются не более чем приближением гиперболы по правой стороне от их моды. Идеальная гипербола может возникнуть только в случае, когда ситуация двух следующих подряд пробелов исключена (устранена).

Очевидно, что, опираясь на данные рис. 2 в рамках гипотезы гиперболического закона распределений длин слов, мы можем перейти к словарю вероятностей Мандельброта по аналогии со словарем для английского языка Ципфа (см. рис. 1).

Таким образом, для оценки энтропии по рассматриваемому варианту критерия Мандельброта нам не хватает только таблицы эмпирических вероятностей реального гиперболического распределения рис. 2. На рис. 3 приведена таблица вероятности, полученная численно, запуском программы, код которой приведен на рис. 2.

Формально мы можем воспользоваться эмпирической таблицей вероятности и вычислить оценку энтропии для различных вариантов коротких последовательностей по следующей формуле (врезка 2).

Приведенная на рис. 3 таблица вероятностей получена на выборке из 9999 примеров псевдослучайных последовательностей. Недостаток числа опытов привел к тому, что в конце таблицы появляются нулевые значения. Это недопустимо при вычислении логарифмов выражения (2). Для выхода из этого вычислительного тупика нули таблицы вероятностей следует заменить на минимальное значение из этой же таблицы: $6{,}39 \cdot 10^{-4}$.

Это позволяет вычислять энтропию для анализируемых случайных последовательностей. На рис. 4 приведено распределение оценок энтропии, полученной для 9999 вариантов псевдослучайных последовательностей.

Из рис. 4 видно, что среднее распределение значений энтропии составляет 31,2 бита, а стандартное отклонение – 9,1 бита. По значениям оценок энтропии рассматриваемого критерия могут быть отброшены кодовые последовательности, наименее похожие на белый шум. Фактически речь идет об устранении «хвостов» распределения.

Подчеркнем, что сумма длин слов из букво-знаков и пробелов между ними должна составлять 55 знаков. Однако конкретное состояние последовательности длин слов этот критерий не способен отследить, поскольку он не чувствителен к перестановкам слов разной длины. В связи с этим значения критерия малы, и данные располагаются в интервале от 8 до 54 бит, что существенно меньше теоретической энтропии Шеннона.

Оценка качества белого шума вторым вариантом критерия Ципфа – Мандельброта

Увеличить значения оценок энтропии удается, если каждое из выделенных слов рассчитать по каждой из знако-букв (исключая три кода, дающих пробел между словами). Так как вероятность появления других кодов одинакова, энтропия слова зависит только от числа кодо-букв n. Тогда энтропия оценивается по следующей формуле (врезка 3).

Распределение значений второго варианта критерия энтропийной оценки Ципфа – Мандельброта приведено на рис. 5.

Из рис. 5 видно, что математическое ожидание откликов второго

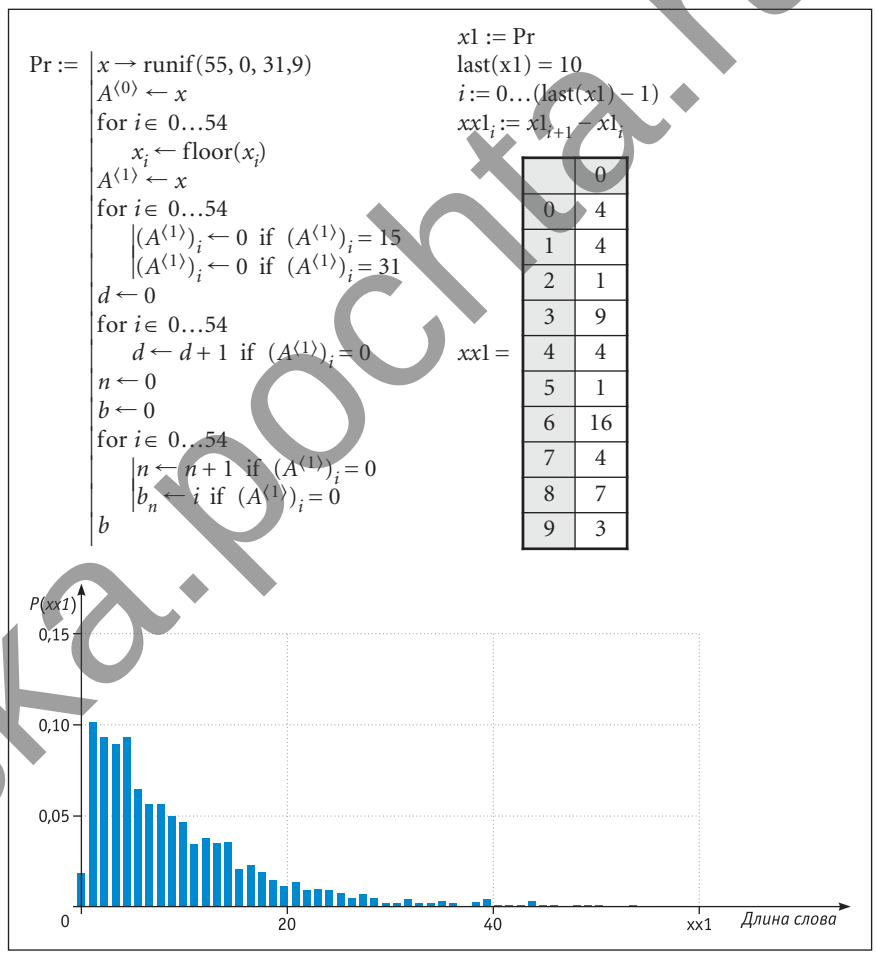


Рис. 2. ***Программная реализация последовательности случайных слов на языке Мандельброта (длина последовательности – 55 букв)***

Врезка 2

$$H(\text{"}x_1, x_2, \ldots, x_{255}\text{"}) \approx -\sum_{i=1}^{N} \log_2(P_i), \qquad (2)$$

где N – число слов, длиной от 0 до 54 букво-знаков, на которое программа левой части рис. 2 разбивает анализируемую ею последовательность.

Врезка 3

$$H(\text{"}x_1, x_2, \ldots, x_{255}\text{"}) \approx -\sum_{i=1}^{N} \log_2(30^{-n_i}) = \sum_{i=1}^{N} 4.907 \cdot n_i, \qquad (3)$$

где n_i – число букв в i-ом слове анализируемой последовательности, а 30 – общее число знако-букв в рассматриваемом варианте случайного языка Мандельброта.

n	P_n	n	P_n	n	P_n	n	P_n
0	0,02	15	0,026	30	$3{,}195 \cdot 10^{-3}$	45	$6{,}39 \cdot 10^{-4}$
1	0,094	16	0,018	31	$1{,}278 \cdot 10^{-3}$	46	$6{,}39 \cdot 10^{-4}$
2	0,09	17	0,014	32	$4{,}473 \cdot 10^{-3}$	47	0
3	0,086	18	0,013	33	$1{,}917 \cdot 10^{-3}$	48	0
4	0,104	19	0,014	34	$6{,}39 \cdot 10^{-3}$	49	$6{,}39 \cdot 10^{-4}$
5	0,065	20	$8{,}307 \cdot 10^{-3}$	35	$1{,}917 \cdot 10^{-3}$	50	0
6	0,061	21	0,012	36	$3{,}834 \cdot 10^{-3}$	51	0
7	0,058	22	$8{,}307 \cdot 10^{-3}$	37	$1{,}278 \cdot 10^{-3}$	52	0
8	0,044	23	$5{,}751 \cdot 10^{-3}$	38	$6{,}39 \cdot 10^{-3}$	53	0
9	0,058	24	$3{,}195 \cdot 10^{-3}$	39	$6{,}39 \cdot 10^{-3}$	54	0
10	0,035	25	$6{,}39 \cdot 10^{-3}$	40	$1{,}917 \cdot 10^{-3}$		
11	0,031	26	$3{,}834 \cdot 10^{-3}$	41	$6{,}39 \cdot 10^{-3}$		
12	0,036	27	$1{,}917 \cdot 10^{-3}$	42	$2{,}556 \cdot 10^{-3}$		
13	0,038	28	$1{,}278 \cdot 10^{-3}$	43	0		
14	0,019	29	$3{,}195 \cdot 10^{-3}$	44	$6{,}39 \cdot 10^{-3}$		

Рис. 3. ***Таблица вероятностей почти-гиперболического закона распределения Ципфа – Мандельброта для случайных 255-битных последовательностей, разбитых на слова длиной от 0 до 54 букво-знаков***

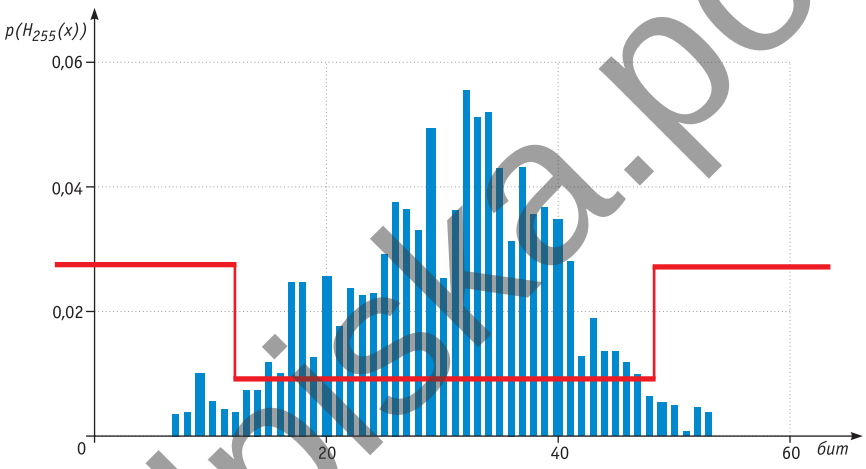


Рис. 4. ***Распределение значений энтропии дробления анализируемой последовательности на букво-знаки***

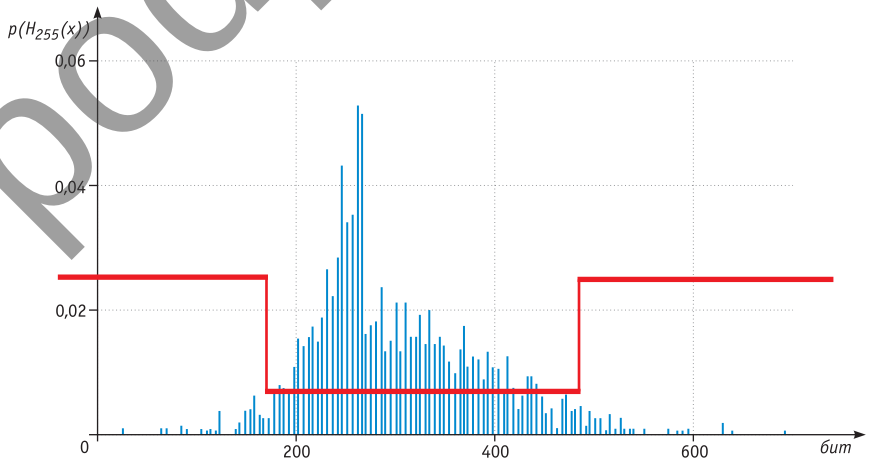


Рис. 5. ***Распределение значений энтропии случайной последовательности выделенных слов, состоящих из разного числа букво-знаков***

варианта критерия увеличивается до значения 300 бит, которое существенно ближе к теоретической энтропии Шеннона в 255 бит для белого шума. Если рассматривать первый критерий для оценки теоретической энтропии Шеннона, то мы получим мультипликативную 8-кратную методическую ошибку [6]. Для второго варианта критерия методическая мультипликативная ошибка снижается до величины 0,85 (наблюдается почти 10-кратное снижение мультипликативной методической ошибки).

Отклики первого и второго вариантов критерия практически не коррелированны. Они хорошо дополняют друг друга при проверке гипотезы белого шума [7]. В связи с этим целесообразно объединять эти два критерия для совместного применения.

Объединение может быть выполнено классическим способом, когда для обоих критериев устранены методические погрешности, а далее данные двух критериев будут нелинейно приведены к одной шкале (например, к шкале энтропии Шеннона). Тогда можно выполнять объединение критериев усреднением их откликов в рамках одной общей шкалы.

Более простым способом объединения критериев является переход к эквивалентным нейросетевым преобразованиям [7]. В этом случае программный код (например, код рис. 2) следует рассматривать как некоторый эквивалент сумматора для персептрона с выходным бинарным квантователем (реализации квантователей приведены на рис. 4 и 5).

Если пороги квантователей подобраны для отсечения 10 % анализируемой выборки, то каждый из двух критериев будет работать с доверительной вероятностью 0,9. Если при анализе выходных данных двух нейронов принимать только состояние «00», то доверительная вероятность решений повышается до 0,99 (следствие низкой коррелированности откликов нейронов).

Заключение

Сегодня существует несколько десятков тестов на случайность (на-

пример, Национальный институт стандартов США (NIST) рекомендует 15 тестов, Дж. Марсельи дает 11 тестов [8, 9]). Эти тесты имеют разную вычислительную сложность: от линейной до экспоненциальной. К сожалению, давно предложенное семейство преобразований Ципфа – Мандельброта (1949–1951 годы) оказалось вне сферы внимания специалистов NIST США. Все преобразования этого типа, с одной стороны, просты и имеют линейную вычислительную сложность, а с другой стороны, их много.

В данной работе рассмотрено формирование пробела между словами дизъюнкцией трех случайно выбранных состояний пятибитных кодировок букв. Любая смена тройки состояний кодов, порождающих пробелы между словами случайных языков Мандельброта, дает новый язык и новый критерий анализа данных на близость к белому шуму. В рассмотренном варианте статьи мы имеем

$$\frac{32!}{3! \cdot (32-3)!} = 4960$$

преобразований. Если мы будем собирать пробелы между словами дизъюнкцией 4-х случайно выбранных кодов, то получим уже

$$\frac{32!}{4! \cdot (32-4)!} = 35\,960$$

вариантов тестов (критериев). Это в сотни и тысячи раз больше размеров списка тестов, рекомендуемого NIST. ■

ЛИТЕРАТУРА

1. Шенон К. Предсказание и энтропия английского печатного текста // Работы по теории информации и кибернетики. – М.: Изд-во иностранной литературы. – 1968. – С. 669–686.

2. Zipf G. K. Human behavior and the principle of least-effort // Cambridge, Ma.: Addison-Westley. 1967 (препринт издания 1949 года, Hefner).

3. Mandelbrot B. B. On the theory of word frequencies and on related Markovian models of discourse // The book: Jacobson R. «Structures of Language and Its Mathematical Aspects». N. Y. American Mathematical Society. 1961.

4. Мандельброт Б. Б., Хадсон З. Л. (НЕ)послушные рынки. Фрактальная революция в финансах. – М.: Вильямс. – 2006. – 400 с.

5. Мандельброт Б. Фрактальная геометрия природы. – М.: Институт компьютерных исследований. – 2002. – 656 с.

6. Иванов А. И., Иванов А. П., Юнин А. П. Устранение методической погрешности оценки энтропии в пространстве расстояний Хэмминга // Защита информации. Инсайд. – 2023. – № 5 (113). – С. 55–59.

7. Иванов А. И. Нейросетевой многокритериальный статистический анализ малых выборок. Проверка гипотезы независимости; справочник // Пенза. – Изд-во Пензенского гос. ун-та. – 2022. – 218 с.

8. Иванов М. А., Чугунков И. В. Глава 4: Методика оценки качества генераторов ПСП // Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-Образ. – 2003. – 240 с.

9. Иванов А. И., Юнин А. П. Эмбрион искусственного интеллекта: компактная нейросетевая проверка качества случайных последовательностей, полученных из биометрических данных. Препринт. – Пенза: Изд-во ПГУ. – 2020. – 48 с.

НОВОСТИ

Объем похищенных персональных данных в РФ вырос более чем наполовину

Экспертно-аналитический центр ГК InfoWatch представил исследование «Россия: утечки информации ограниченного доступа, 2022–2023 годы», в котором подробно проанализировал характер и динамику инцидентов ИБ в России за последние два года.

Согласно отчету, в 2023 году произошел резкий рост количества утекших ПДн: их объем составил 1,12 млрд записей, что почти на 60 % выше уровня 2022 года. Причем истинный масштаб ущерба может быть существенно недооценен, поскольку более чем в 35 % прошлогодних утечек объем украденных данных остался неизвестен. Среднее количество ПДн, «слитых» за один инцидент, в 2023 году увеличилось почти вдвое: с 0,9 до 1,7 млн записей.

По словам экспертов, данный тренд, в первую очередь, связан с появлением крупных хранилищ ПДн (относящихся к социальным сервисам, операторам связи, маркетплейсам и т. д.) на фоне ускоренной цифровизации экономики. В настоящее время именно они становятся основными мишенями для кибератак. Ожидается, что в скором будущем к ним добавятся и хранилища, относящиеся к федеральным сервисам, которые станут желанной целью для злоумышленников с политической мотивацией. Поэтому базы данных госсервисов требуют особенно тщательной защиты.

Активизацию атак на организации госсектора можно заметить уже сейчас, например, по динамике доли утечек сведений, содержащих гостайну, возросших в 2023 году с 1,8 до 6,6 %. Увеличилась и общая доля информации, утекшей из государственных органов и организаций – до уровня в 19,2 % (на 5,3 % больше по сравнению с 2022 годом). Одновременно с этим в зоне снижения оказались компании, работающие в сфере ИТ/ИБ и телекоммуникаций (с 27,1 % в 2022 году до 18,8 % в 2023-м) и торговых организаций (с 19,6 до 16,6 %).

Произошло также значительное увеличение доли ИП в общем объеме похищенных ПДн и компаний малого бизнеса (до 50 сотрудников) с 18,5 до 34,1 % за счет равномерного снижения долей крупных и средних игроков рынка.

Согласно данным опроса ГК InfoWatch, в ответ на ухудшение ситуации с утечками конфиденциальной информации организации задействовали следующие основные меры укрепления кибербезопасности: обучение сотрудников основам ИБ (59 %), внедрение системы защиты от вторжений (27 %) и установка DLP-системы (17 %).

infowatch.ru

Расшифровка утерянных писем Марии Стюарт 1578–1584 годов. Часть 5

En **Deciphering Mary Stuart's Lost Letters from 1578–1584. Part 5**

George Lasry
george.lasry@gmail.com
University of Kassel

Norbert Biermann
n.biermann@udk-berlin.de
Berlin University of Arts

Satoshi Tomokiyo
verlat@hotmail.com
University of Tokyo

This publication is the final part of the cycle, which is a translation of the research report (the results were published in the journal Cryptologia in early 2023) discovered by a group of scientists in the archives of the Bibliothèque Nationale de France collection of previously unknown encrypted letters of Mary I Stuart, Queen of Scots, written in the years preceding her execution in 1587, addressed mostly to Michel de Castelnau, the French ambassador to England.

Keywords: cryptography, deciphering, Mary Stuart, Michel de Castelnau, secret communication channels, codebreaking algorithm, encryption errors

УДК 930.253

Настоящий материал является заключительной частью цикла публикаций[1], представляющих собой перевод отчета по исследованию (результаты были опубликованы в журнале Cryptologia в начале 2023 года[2]) обнаруженной группой ученых в архивах Национальной библиотеки Франции коллекции неизвестных ранее зашифрованных писем королевы Шотландии Марии I Стюарт, написанных в годы, предшествовавшие ее казни в 1587 году, и адресованных, главным образом, французскому послу в Англии Мишелю де Кастельно.

Ключевые слова: криптография, дешифрование, Мария Стюарт, Мишель де Кастельно, секретные каналы связи, алгоритм взлома кода, ошибки шифрования

Джордж Лэсри
george.lasry@gmail.com
Кассельский университет

Норберт Бирманн
n.biermann@udk-berlin.de
Берлинский университет искусств

Сатоси Томокиё
verlat@hotmail.com
Токийский университет

6. Секретные каналы связи Марии Стюарт

Для историков существование секретного канала связи между Марией и Кастельно давно не являлось тайной, более того, об этом было известно даже английскому правительству того времени (см., например, [2]). Несмотря на это, Босси утверждает, что до середины 1583 года канал был настолько защищен, что его содержимое казалось утерянным [2]. Наша работа доказывает, что такой канал существовал, минимум, с мая 1578 года. Кроме того, хотя некоторые связанные с ним детали были известны и ранее, новые расшифровки заметно дополняют имевшиеся сведения как о его функционировании, так и о вовлеченных в этот процесс людях.

6.1. Официальные и секретные каналы

Во время содержания в плену Марии разрешалось писать и получать письма официальной почтой, которую она называла обычной почтой, почтой Уолсингема и т. п.[3] Впрочем, иногда, по указанию Уолсингема, доставку писем значительно за-

[1] *Начало см. в №№ 2–6'2023.*
[2] *George Lasry, Norbert Biermann & Satoshi Tomokiyo (2023): Deciphering Mary Stuart's lost letters from 1578-1584 // Cryptologia. – DOI: 10.1080/01611194.2022.2160677.*
[3] *Например, «par la voye ordinaire» (Мария – Битону от 4 июля 1579 года [4] и Мария – Кастельно от 22 и 25 июля 1583 года (BL Harleian MS 1582/306, воспроизведено в [4]).*

держивали (F82, F125, F247, F64)[4], а то и вовсе запрещали переписку[5]. Помимо обращений к королеве Елизавете или к ее представителям официальный канал использовался и для других нужд, например, для управления собственностью Марии во Франции [2]. В нескольких письмах, которые мы расшифровали, она прямо пишет, что официальные письма не содержат ничего такого, что требовалось бы хранить в секрете даже от своих врагов (F74, F231). В свое время Мария даже разрешила Archibaldu Дугласу писать ей по этому каналу о незначительных вещах[6].

В дополнение к официальному каналу Марии удавалось поддерживать секретную переписку по конфиденциальным каналам, упоминаемым в ее письмах как *la voye secrete* (секретная почта) или просто *ceste voye/commodité* (эта почта/удобство, комфорт). Письмо может считаться конфиденциальным и, следовательно, отправленным в зашифрованном виде, если в нем упоминается такая *voye* или содержится ссылка на другое секретное письмо (или, само собой разумеется, на какое-либо иное конфиденциальное содержание), даже если в архивах сохранилась только открытая копия этого письма[7]. Гораздо сложнее с уверенностью утверждать, что имеющееся в архивах конкретное письмо с открытым текстом изначально не отправлялось в зашифрованном виде[8].

Расшифрованные нами письма содержат дополнительные прямые ссылки на такие каналы, которые ясно указывают на то, что конфиденциальные каналы действовали параллельно с официальным (F153),

Источник: https://en.wikipedia.org/

Сеньор Ретрадо де Бернардино де Мендоса (1540–1604) (неизвестный художник)

и Мария иногда использовала официальный канал для несущественных вопросов (F165), в тот же день отправляя зашифрованное письмо с другим содержанием (F174). Например, в период подготовки вояжа де ла Мот-Фенелона в Шотландию в конце 1582 года Мария не только направляла ему секретную корреспонденцию через Кастельно, но и писала по официальному каналу во избежание каких-либо подозрений (F123).

Письма, переправляемые по секретным каналам, были не застрахованы от перехвата или, возможно, от случайных любопытных глаз носителя. Поэтому, когда Мария узнала о намерении Кастельно искать помощи у Екатерины Медичи, она попросила его передать привет королеве-матери и извиниться за то, что не обращается к ней сама[9], поскольку не осмеливается отправить что-либо незашифрованное (Екатерине Медичи) «этой почтой» (*par ceste voye*) вместе с зашифрованным письмом Кастельно (F54). Нау выразил свое разочарование по тому же поводу в постскриптуме, сказав, что хотел ответить некоему Фостеру, но не рискнул передавать незашифрованное послание по секретному каналу (F89).

Наши расшифровки выявили один инцидент, в ходе которого Кастельно действовал весьма неосмотрительно, переслав зашифрованное письмо от Битона в пакете, отправленном по официальному каналу. К счастью, Шрусбери, вскрывший пакет, не потрудился изучить его содержимое и, по-видимому, не заметил зашифрованного письма. Мария посоветовала послу впредь быть осторожнее (F50).

Известно, что Кастельно пересылал конфиденциальную переписку между Марией и ее партнерами в континентальной Европе, такими как проживавший в Париже Битон. Дипломатическая почта была самым безопасным средством избежать ее перехвата в портах [1, 2, 8][10].

Известно также, что Бернардино де Мендоса, посол Испании в Лондоне, переслал Битону, по крайней мере, одно письмо от Марии[11]. Что касается доставки ее писем испанскому послу в июне 1583 года, Мария упоминает опасный канал связи через предшественника де Мендосы[12] (F113).

---

[4] *См. также CSP Scotland, v. 5, № 225.*

[5] *Мария – Кастельно от 8 октября 1582 года (BnF Fr.3181/f.9, воспроизведено в [4]).*

[6] *Мария – Кастельно от 3 сентября 1583 года (Hatfield Cecil Papers, 133/31; Hatfield Calendar, 13/234; F69, воспроизведено в [4]).*

[7] *Можно было бы ожидать, что письма, поступившие через завербованного Уолсингемом крота во французском посольстве (см. раздел 6.4) – секретные, поскольку, очевидно, нет необходимости в тайной передаче содержания писем, отправленных открытым текстом по официальному каналу. Однако неожиданно в Add MS 48049 содержатся копии двух писем, сделанные рукой Ферона, оригиналы которых (от 2 января и от 22 марта 1584 года) в открытом виде хранятся во французских архивах, то есть считаются отправленными по официальному каналу (приведены в [4]). Вероятно, крот не потрудился разобраться или у него не было на это времени, какие письма являются официальными и потому, вероятно, и так известны Уолсингему, а какие нет.*

[8] *Когда в архивах имеется только копия письма с открытым текстом, не всегда очевидно, что она сделана с изначально открытого текста, а не с расшифрованного, если только копия не является оригиналом с автографом, обычно помеченным как «original» в [4]).*

[9] *Письмо Марии от 15 августа 1585 года, единственное в этот период, адресованное ею Екатерине Медичи, является автографом [4].*

[10] *Мария – Битону от 20 февраля 1576 и от 21 мая и от 1 июня 1576 (воспроизведено в [4]).*

[11] *Мария – Битону от 7 апреля 1582 года (воспроизведено в [4]).*

[12] *Возможно, формулировка Марии направлена на то, чтобы скрыть от Кастельно существование ее секретного канала связи с испанским послом.*

6.2. Доставка и перехват писем

Марии пришлось столкнуться с многочисленными трудностями в ходе поддержания безопасного секретного канала связи с внешним миром, в том числе с Кастельно, даже несмотря на то, что бдительность Шрусбери иногда ослабевала[13]. Однажды она обмолвилась в письме о том, что отправлять кого-либо, кто доставит ее корреспонденцию напрямую адресату, весьма рискованно. Безопаснее использовать Лондон в качестве промежуточной инстанции, поскольку там у нее имеются друзья, в отношении которых она уверена, что они доставят письма в целости и сохранности[14].

Секретные письма Марии часто перехватывались, в том числе на пути из ее резиденции [3]. Иногда надежную доставку отправленных ею посланий нельзя было гарантировать, и они возвращались ей обратно. Одно из таких писем дважды доходило до Лондона, но в связи с невозможностью передачи адресату вернулось почти через два месяца после отправки. Получив его, Мария сначала захотела обновить содержание, включив туда последние новости, но удовлетворилась очередной отправкой, потому что курьер не мог ждать (F82). В итоге посыльный, ощутив неминуемое разоблачение, сжег письмо. То же самое произошло с посылкой, доверенной Джоном Гамильтоном некоему Джексону для доставки Моргану, в то время находившемуся в Лондоне[15].

Входящие письма также задерживались. Иногда они доставлялись после прочтения, но зашифрованные всегда конфисковывались [9][16]. В отсутствие доступных средств безопасной доставки отправления для Марии накапливались во французском посольстве [2, 8].

Источник: https://artuk.org/
Сэр Эмиас Паулет (1532–1588) (неизвестный художник)

Иногда узнице разрешались посещения ее сподвижников, которые в некоторых случаях имели с собой предназначенные ей письма или разносили письма Марии по другим адресатам. Например, когда Эндрю Битон, брат Джеймса Битона, был отправлен во Францию, он привез с собой секретные письма для ее родственников [9]. Конечно, в таких случаях были необходимы предельные меры предосторожности[17]. Так, дю Рюссо удалось передать Марии при посещении привезенные с собой письма, но на обратном пути он был задержан Шрусбери, и письма Марии – конфискованы [5, 9][18]. Одно из расшифрованных нами писем (F118) содержит жалобы Марии на арест дю Рюссо.

Однако посетителей пускали не всегда. В 1581 году просьба Марии послать за врачами была встречена неодобрительно ввиду подозрения, что она попытается связаться через этих врачей с герцогом Анжуйским, который, как ожидалось, нанесет визит в Лондоне королеве Елизавете [5][19]. Даже пристальное наблюдение за такими встречами не могло полностью исключить обмен посланиями между Марией и посетителями [5, 9].

В 1585 году Мария находилась под более строгой опекой сэра Эмиаса Паулета, который, узнав, что кучера и прачки могут перевозить ее письма, принял строгие меры, чтобы предотвратить это [7].

6.3. Меры предосторожности

Мария очень заботилась о том, чтобы ее секретный канал связи с Кастельно не был раскрыт.

В 1583 году она хотела доставить таблицу шифров Арчибальду Дугласу через Кастельно, но, чтобы скрыть существование своего секретного канала связи с французским посольством, попросила последнего отложить доставку Дугласу до тех пор, пока некие женщины (вероятно, ее служанки), посещавшие посольство, не покинут Лондон. Эта предосторожность не позволила бы Дугласу вызнать у них, что шифровальная таблица поступила именно от Марии, а не от посла. Она также попросила Кастельно убедить Дугласа в том, что все написанное последним с использованием шифра будет пересылаться обычной почтой[20].

Расшифрованные нами письма также содержат упоминания о подобных мерах предосторожности.

Когда дю Рюссо сразу после посещения Марии был арестован в Шеффилде, в доме Шрусбери, она попросила Кастельно заявить протест королеве и Уолсингему. При этом, резонно предположив, что арест производился тайно, она проинструктировала Кастельно сослаться на то, что он не получал известий от дю Рюссо в течение двух месяцев, хотя тот говорил ему о намерении остать-

[13] *В марте 1575 года Шрусбери доложил лорду Берли: «What intellygens passeth for this Quene to and fro my house I doo not know» (Я не знаю, какие сведения проходят через эту королеву в мой дом и из него) [3].*
[14] *Мария – Битону (июнь 1574 года) (воспроизведено в [4]).*
[15] *Мария – Битону от 20 февраля 1576 года (воспроизведено в [4]).*
[16] *В источнике содержится ссылка на письмо Шрусбери и Хантингдона Сесилу от 19 декабря 1569 года, хранящееся в State Paper Office (Государственная канцелярия – основанное в 1578 году в Лондоне хранилище важных правительственных документов. – Примеч. ред.).*
[17] *Андре – Битону от 22 августа 1577 года (воспроизведено в [4]).*
[18] *Мария – Кастельно от 8 октября 1582 года (BnF Fr.3181/f.9, воспроизведено в [4]). См. также сноску к F74 в разделе 5.3, касающуюся письма дю Рюссо.*
[19] *В источнике цитируется письмо Била Уолсингему от 23 ноября 1581 года (SP53/11/69).*
[20] *F78. Также в Hatfield Calendar v. 3, 12 (Cecil Papers, v. 162, p. 23–24).*

ся в Шеффилде всего на три недели. Таким образом, мол, он и пришел к выводу об удерживании дю Рюссо против воли последнего (F118 от 24 сентября 1582 года).

После того как дю Рюссо был освобожден, Мария попросила Кастельно не пересылать вложение Битону до получения первым известия о том, что дю Рюссо достиг Кале. Цель задержки, очевидно, заключалась в создании впечатления, будто письмо Битону доставил именно дю Рюссо (F245 от 13 октября 1582 года).

В другой раз Мария попросила Кастельно передать от нее слова благодарности Билю, но упомянуть при этом, что слова Марии стали известны ему от дю Рюссо после посещения тем Шеффилда (F153 от 15 января 1583 года).

Были и другие случаи, когда Мария просила Кастельно предоставить королеве Елизавете или лорду Берли некоторую информацию, не сообщая им, откуда на самом деле она исходит (F21, F64, F89).

6.4. Тайные курьеры

Конфиденциальными каналами связи Марии в течение многих лет ее пребывания в плену управляли несколько человек.

Некий Синглтон отвечал за секретную переписку Марии на протяжении семи или восьми лет, но в сентябре 1580 года ему пришлось покинуть Англию ввиду ужесточения контроля над католиками в этой стране. Этот Синглтон и упомянутый в нескольких расшифрованных нами письмах Робертсон, по-видимому, являются одним и тем же лицом[21].

Проблемы с доставкой писем у Робертсона возникли, скорее всего, за несколько месяцев до того, как Мария написала в мае 1578 года о своем беспокойстве по поводу отсутствия корреспонденции от Кастельно или из Франции в течение последних семи или восьми месяцев. Чтобы показать Робертсону, что она не преминет возместить ему ущерб, она прислала ему цепочку с драгоценными камнями (F87). Неприятности Робертсона и, следовательно, прерывание канала связи с Марией, возможно, как-то связаны с (предполагаемым) раскрытием некоторых из ее сподвижников в Англии, о чем сообщал Томас Морган 25 декабря 1577 года[22]. Когда Мария написала Кастельно, что ей пришлось искать альтернативные способы доставки писем, поскольку нанятый ею человек оказался недоступен (F241), она, вероятно, имела в виду именно Робертсона.

Постоянно велась работа по набору новых курьеров. При этом предпринимались меры предосторожности: первоначально новичку поручали передачу сообщений, не относящихся к разряду конфиденциальных[23]. В октябре 1579 года (F249) Нау отправил Арно записку через некого «блюстителя закона» (F179), в которой просил своего коллегу написать ему по некоторым незначительным вопросам, чтобы убедиться в надежности посыльного. В следующем месяце Мария, возможно, ссылалась на этого же курьера, когда писала «*ceste voye que je n'ay encores bien experimentée*» (к сожалению, я еще недостаточно хорошо проверила этот канал), и поэтому воздержалась от упоминания деликатных вопросов даже в зашифрованном письме (F233).

Иногда Марии, чтобы передать секретное письмо, все же приходилось полагаться на кого-то, кому она не могла полностью доверять, например, на слугу графини Шрусбери. В передаваемом с ним письме содержится просьба к Кастельно не раскрывать ничего важного этому человеку, так как он, возможно, сообщит Лестеру обо всем, что узнает (F308). В январе 1580 года (F181) Мария написала Кастельно, что пробует «*voye nouvelle*» (новый канал). В 1581 году Годфри Фолджамб (Foljambe)[24] упоминался как человек, который всегда мог предоставить курьерскую службу «по умолчанию для всех», когда «эта почта» недоступна (F82, F235). В апреле 1582 года Мария упомянула в письме Кастельно имя Безет и попросила посла попытаться наладить через него канал для доставки ее писем в Шотландию, но только в том случае, если это тот самый Патрик Безет, которого она знала (F165).

Клод де Курсель, секретарь Кастельно, занимался доставкой корреспонденции и контролировал секретный канал связи примерно с конца 1581 года. Он встречался с людьми Марии, имел контакты в Лондоне и тесно сотрудничал с ее партией в Париже [2].

В середине 1583 года Уолсингему, наконец, удалось проникнуть в секретный канал связи между Марией и Кастельно, завербовав шпиона во французском посольстве. Долгое время считалось, что шпионом, снабжавшим Уолсингема копиями их переписки, являлся некий Шереллес. Основанием тому послужил пост-

[21] *Между Робертсоном, упомянутым в наших расшифрованных письмах, и Синглтоном, упомянутым в письмах к Битону, и воспроизведенных в [4], имеется определенное сходство. Во-первых, Мария считает, что Робертсону лучше всего уехать во Францию из-за «жестоких преследований» католиков (F237 от 16 сентября 1580 года), а в письме к Битону от 27 сентября 1580 года [4] упоминается, что предъявитель сего решил пересечь море из-за «жестоких преследований» католиков, посему он и рекомендуется Битону. Далее в том же F237 Мария просит Битона «выдать 500 экю этому предъявителю», то есть Робертсону , в то время как в другом письме она благодарит Битона за выданные Синглтону 500 экю [4]. Во-вторых, как в F239 от 27 сентября 1580 года, так и в вышеупомянутом письме Битону из [4] среди прочего говорится о пенсионе и представлении королю герцогом де Гизом. В-третьих, вложение для Синглтона в письме Битону было помечено символом «Т» [4], как и вложения для Робертсона в письмах Кастельно F237 и F181. Та же система маркировки вложений использовалась в письмах Марии, адресованных Битону и Кастельно, например, в F21 и F185).*

[22] *«Есть сведения (согласно некоторым письмам Ее Величества, направленным милорду Сетону во Фландрию), что некоторые из ее лучших слуг в Англии раскрыты и, таким образом, теперь вынуждены, как они говорят, принять участие в моем изгнании» (Морган графине Нортумберленд, CSP Scotland). Также в F87 Робертсон, кажется, обеспокоен перехватом писем Марии Сетону во Фландрию, но узница утверждает, что не писала тому с момента его отъезда.*

[23] *Чарльз Пейджет – Марии Стюарт от 17 июля 1585 года (TNA SP 53/16/15).*

[24] *Также пишется Fullgham или Foulgiam. Зашифрованное письмо Марии в TNA SP53/18/64 с пометкой «Расшифровано 21 июля 1586 года» адресовано «To Fulgeam».*

скриптум, добавленный к одному из таких писем. Босси пришел к другому выводу и предположил, что кротом был вовсе не Шереллес, которого он идентифицировал как Жана Арно, а клерк посольства Лоран Ферон [2, 4].

Одним из контактов Курселя в Лондоне был сэр Фрэнсис Трокмортон [2], изначально завербованный Синглтоном в мае 1581 года, а затем познакомившийся в Париже с агентами Марии, такими как Томас Морган и Чарльз Пейджет[25]. В письме от апреля 1582 года (F125), после того как несколько ее отправлений были задержаны, Мария представила Трокмортона Кастельно. Трокмортон сблизился с послом, занялся переправкой писем, но в ноябре 1583 года был арестован после раскрытия заговора, известного в истории под его именем. Скорее всего, именно в результате его ареста было перехвачено письмо Кастельно к Марии от 5 ноября 1583 года, которое сохранилось только в копии, написанной рукой Фелиппеса. Вполне вероятно, что Кастельно использовал в своих письмах к Марии тот же шифр, что и она в письмах к нему, а это наводит на мысль, что шифр либо был взломан Фелиппесом, либо утек через Ферона[26].

После раскрытия заговора Трокмортона Мария, сожалея «об обнаружении всех моих контактов, которые часто бывали в вашем доме», заподозрила, что в посольстве окопался шпион, и попросила Кастельно, чтобы ее посланцев принимали где-нибудь вне пределов его ведомства, причем исключительно те люди, чья лояльность гарантирована. В ответ Кастельно заверил ее, что только три человека в посольстве знают об их секретной переписке. К сожалению, среди этих троих был Ферон, которого Кастельно не подозревал в причастности к утечке, потому что он «никогда не выходит из моей комнаты и все записи делает передо мной и в моем присутствии». Двумя другими были Курсель и Арно [2].

Мария, кстати, еще в январе 1583 года обращалась к Кастельно со схожими советами (F247):

- курьеры не должны знать друг друга;
- никому, помимо Кастельно, не желательно знать, кто является текущим курьером;
- тем сотрудникам посольства, кто уже в курсе дела, следует соблюдать абсолютную секретность.

Еще один курьер, Томас Болдуин, был лондонским представителем графа Шрусбери и занимался перевозками между Лондоном и Шеффилдом. Он был завербован Курселем и доставлял письма Марии, минимум, с октября 1581 года (F194). Так, в феврале 1583 года Болдуин должен был привезти в Шеффилд 2000 экю (F174). Даже после ареста Трокмортона ему удавалось доставлять конфиденциальные письма Марии вплоть до собственного ареста в октябре 1584 года [2].

Раскрытие заговора Трокмортона в ноябре 1583 года поставило Кастельно в щекотливое положение. Ему пришлось пообещать Уолсингему, что он покажет ему все письма к Марии и от нее, хотя непосредственно перед тем, как дать обещание, он отправил той пакет с письмами, которые скопились в посольстве. Тем временем обширные неформальные связи посла с Марией вызвали вопросы при французском дворе [2], вследствие чего Кастельно был отозван в ноябре 1584 года и в следующем году покинул Англию.

С заменой Кастельно Гийомом де Л'Обеспином, бароном де Шатонеф, похоже, Мария прекратила переписку по официальному каналу под наблюдением Уолсингема[27]. Часть переписки между Марией и Шатонефом хранится в британских архивах, причем некоторые экземпляры написаны рукой Фелиппеса. Это позволяет предположить, что их конфиденциальные письма перехватывались и расшифровывались английскими властями. Существует даже послание Уолсингема Фелиппесу, приложенное к перехваченным письмам д'Эсневаля и Шатонефа, в котором он просит криптографа выяснить их содержание[28]. Все эти письма относятся к периоду, когда Марию убедили в том, что Гиффорд, который на самом деле был двойным агентом Уолсингема, установил безопасный канал связи (см. раздел 2).

6.5. Кодовые имена и псевдонимы

В секретной переписке Марии с Кастельно зашифрован был не только текст, но для дополнительной безопасности использовались и некоторые кодовые имена или псевдонимы. Например, *M. de la Tour* или *Sieur de la Tour* относились к Фрэнсису Трокмортону. Идентификация его личности очевидна для историков, поэтому Босси предполагает, что об этом знал в том числе и Уолсингем [2][29]. В пись-

[25] *Мария – Битону от 27 сентября 1580 года и Мария – Битону от 20 мая 1581 года (воспроизведены в [4]).*

[26] *Письмо находится в TNA SP53/12/92. О захвате см. [2]. О возможной утечке шифровальной таблицы через Ферона: в мае 1583 года агент Уолсингема «Фагот» написал ему: «Я подружился с секретарем посла, и если ему передадут определенную сумму денег, он будет сообщать мне обо всем, что ему поручено, в том числе связанное с королевой шотландцев, и шифре, который ею используется» [1, 2]. В любом случае, мы рассчитывали найти копию воссозданного ключа шифрования в британских архивах, но нам это не удалось. Зато мы обнаружили очень короткий нерасшифрованный фрагмент шифртекста на полях черновика письма Кастельно Марии, датированного Босси [2] 14/24 декабря 1583 года (BL Harley MS 1582, f.385). Он расшифровывается как «monsieur… monsieur Nau trouvera», «madame … madame pour ja la» («месье… месье Нау найдет», «мадам… мадам для вас»). Казалось бы, соответствующий открытый текст находится в предпоследней строке f.373r (март 1584): «…madame. Monsieur Nau trouvera icy…» («…мадам. Месье Нау найдет здесь…»). Возможная интерпретация заключается в том, что зашифрованный текст на полях был нацарапан в 1584 году на черновике 1583 года. Однако неясно, кто написал эти каракули.*

[27] *Известно более 10 писем Марии к Кастельно, написанных открытым текстом в период с весны 1584 по ноябрь 1585 года и предположительно отправленных под наблюдением Уолсингема. Все они находятся во французских архивах. Однако писем Шатонефу (отправленных открытым текстом), относящихся к тому времени, когда последний был послом в Англии, там нет.*

[28] *Уолсингем – Фелиппесу от 3 сентября 1586 года (TNA SP53/19/80).*

[29] *Этот псевдоним используется в письмах Кастельно к Марии с 1583 года [2], письмах Марии к Кастельно от 1584 года [4] и в расшифрованных нами письмах F125, F174, F130, F89, F34, F78, F58.*

ме от 25 февраля 1584 года даже содержится прямая ссылка: оно адресуется «*du Sieur de la Tour, du Comte de Northumberland et de mylord Henry Hovard*», а несколькими строками ниже слова «*ledict Throkmorton et Hovard*» связывают псевдоним *Sieur de la Tour* с Трокмортоном[30]. В одном из писем, которые мы расшифровали, Мария недвусмысленно вводит упомянутое кодовое наименование: «*ce gentilhome qui s'apellera entre nous 'la Tour'*» (этот джентльмен, которого между нами будем называть '*la Tour*') (F125, 7 апреля 1582 года).

Генри Говарду, упомянутому вместе с Трокмортоном в приведенной выше цитате, также был присвоен псевдоним. Мария называла его *mon frere* (мой брат), Кастельно – *vostre frere* (твой брат)[31], а Нау – *le frere de la royne d'Escosse* (брат королевы Шотландии) (F74) или *le frere de Sa Majestй* (брат Ее Величества) (F225). По словам Босси, псевдоним вытекает из намерения Марии выйти замуж за брата Говарда – герцога Норфолка [2]. Поэтому Мария называла племянников Говарда, то есть сыновей Норфолка, «своими детьми» [11]. Самое раннее обнаруженное нами использование этого псевдонима относится к F74 (октябрь 1582 года)[32], где Нау предложил новый символ для Говарда, который, впрочем, не использовался ни в одном из последующих рассмотренных нами зашифрованных текстов. Фамилия «Говард» открыто написана в F158 (июль 1582), F245 (октябрь 1582) и F58 (февраль 1584). Псевдоним frere, возможно, был введен в октябре 1582 года и вышел из употребления после ареста Говарда в конце 1583 года.

Известны и другие псевдонимы: по словам Босси, *Monsieur de la Rue* – это псевдоним тайного слуги Марии – иезуита Анри де Самери, а *Banque*, возможно, был Болдуином[33]. Робертсон, о котором мы писали в разделе 6.4, мог являться кодовым именем для Синглтона, или наоборот.

7. Заключение

Тот факт, что письма были полностью зашифрованы и хранились в архивных коллекциях вместе с несвязанными материалами и неполной каталожной информацией, может объяснить, почему эти документы ранее не приписывались Марии Стюарт[34]. Таким образом, настоящая работа была бы невозможна без предварительных систематических усилий по картографированию, оцифровке и расшифровке писем, хранящихся в архивах, выполненных с помощью проекта DECRYPT и web-сайта Cryptiana [6, 10].

Возможно, изучение других коллекций в BnF и прочих архивах приведет к обнаружению по-прежнему неизвестных зашифрованных документов Марии Стюарт. Вероятность этого достаточно высока, если учесть, что у нас имелся доступ только к онлайн-коллекциям BnF, а также принять во внимание наличие доказательств существования ряда доселе необнаруженных зашифрованных писем[35]. Кроме того, более тщательное изучение физических документов в коллекциях, охватываемых настоящей работой, сможет помочь в заполнении некоторых пробелов в расшифрованных текстах, вызванных низким качеством сканов или самих документов, а также позволит исследовать такие параметры последних, как чернила, бумага и почерк. Интересно будет также понять, почему почти все зашифрованные документы оказались, в основном, в несвязанных коллекциях BnF.

В [1, 2] Босси приводит подробный отчет о том, как Уолсингем и его агенты проникли в посольство Кастельно в середине 1583 года и скомпрометировали секретный канал связи Мария – Кастельно, а через последнего – канал связи с их соратниками и союзниками, главным образом, во Франции. Настоящая работа подтверждает гипотезу Босси о том, что указанный секретный канал к середине 1583 года уже существовал на протяжении некоторого времени, показывая, что он был создан еще в 1578 году и наиболее активно использовался в 1582 и 1583 годах.

Расшифрованные письма также свидетельствуют о неустанных усилиях по набору курьеров и обес-

[30] *F58, также в [4]. Босси считает, что идентификация, вероятно, осуществлена скопировавшим письмо Фероном [2]. Видимо, его мнение основывается на предположении, что Ферон изобразил один и тот же символ как «Sieur de la Tour» в одном месте и как «Трокмортон» – в другом. Однако наша расшифровка F58 показывает, что это не тот случай. В зашифрованном тексте написано «de la Tour», а затем «Трокмортон». Различие в символах не было зафиксировано Фероном, но оно есть в исходном зашифрованном тексте.*

[31] *Один из примеров, приведенных Босси [2], соответствует F46. Слова «mon frere» в F46, а также в копии этого письма из Harleian MS 1852, соответствуют пропущенному тексту в версии д'Эшевраля (см. сноску к F46 в разделе 5.3).*

[32] *Другие варианты использования найдены в F30, F34, F46, F78, F89 и F113.*

[33] *В [2] упоминается псевдоним «Renous Banque», основанный на предложении «Le porteur s'appellera cy a present Renous Banque» (Предъявитель сего отныне будет называться «Известный банк») из открытой копии расшифрованного письма Курселю [4]. Это, по-видимому, ошибка дешифрования, поскольку последовательность расшифрованных букв имеет больший смысл, если их разделить на слова следующим образом: «Le porteur s'appellera cyapres entre nous Banque» (Предъявитель сего отныне будет называться между нами «Банк»). То есть псевдонимом является «Банк», а не «Известный банк». С такой трудностью часто сталкиваются при прочтении шифртекста, записанного без разрывов между словами.*

[34] *Сначала мы расшифровали исходный набор писем (BnF fr. 2988), и только после осознания их значения, нами были предприняты согласованные усилия по поиску других писем, зашифрованных теми же графическими символами. Начав с коллекций BnF, которые, как было известно, содержат документы Кастельно, мы нашли еще два зашифрованных письма в BnF Cinq Cents de Colbert 470 (F307, F308) и что более важно, письмо в BnF fr. 3158 (F57) от Марии Стюарт к Кастельно, написанное в основном открытым текстом, но с некоторыми зашифрованными отрывками. Лабаноффу было известно об этом письме, воспроизведенном им в [4] без зашифрованных частей, и поскольку он также изучал связанные с Марией Стюарт документы из архива Кастельно в коллекции BnF Cinq Cents de Colbert 470, теоретически он мог бы сделать вывод, что зашифрованные письма в этой коллекции (F307, F308) также написаны ею. Кроме того, такой вывод, возможно, позволил бы ученому, изучавшему содержимое BnF fr. 2988, признать, что автором имеющихся там писем также была Мария.*

[35] *В частности, за 1578–1581 годы (см. раздел 5.1).*

печению секретности и безопасности связи, предпринимавшихся Марией и ее соратниками. К сожалению, нам не удалось установить, кто именно шифровал письма Марии, хотя мы смогли наблюдать некоторое разнообразие в почерках и выборе конкретных омофонов для шифрования. Дальнейшие исследования, включая сравнительный анализ почерка, в сочетании с такими инструментами, как статистический анализ, возможно, позволят идентифицировать конкретных лиц, выполнявших эту работу для шотландской королевы[36].

Еще одно направление для дальнейших исследований связано с ролью исторического взлома кодов в отношении переписки Марии – Кастельно. Хотя, по крайней мере, одно их письмо, по-видимому, было перехвачено и расшифровано Фелиппесом в конце 1583 года[37], мы не нашли ключа к используемому ими шифру среди десятков связанных с Марией ключей шифрования, хранящихся в британских архивах, а также не обнаружили в последних ни одного документа, зашифрованного этим шифром.

Хотя мы подробно рассмотрели в этой статье коммуникации Марии, существует множество других тем, по которым при дальнейшем изучении расшифрованных документов могут быть получены новые сведения, относящиеся к конкретным событиям или людям[38]. Другим возможным направлением будущих исследований могло бы стать систематическое сравнение стиля письма, структуры и тематики зашифрованных писем с незашифрованными письмами, которые в основном отправлялись по официальным каналам.

Из-за огромного объема расшифрованного материала, в общей сложности около 50 000 слов, которого достаточно, чтобы заполнить целую книгу, в настоящей публикации мы ограничились в основном лишь предварительными резюме писем, и только некоторые из них воспроизвели полностью. Тем самым мы надеемся предоставить историкам, обладающим соответствующими знаниями, достаточный стимул для углубленного изучения их содержания, чтобы извлечь оттуда информацию, которая обогатила бы наш взгляд на содержание в плену Марии Стюарт в 1578–1584 годах.

Ученые, заинтересованные в получении доступа к расшифрованным материалам, могут связаться с авторами. Со своей стороны, авторы заинтересованы в сотрудничестве с учеными для подготовки аннотированного издания всех недавно расшифрованных писем.

Приложение А. Алгоритм взлома кода

Принцип, лежащий в основе алгоритма взлома кода, заключается в преобразовании задачи восстановления ключа только из зашифрованного текста в задачу оптимизации. Для этого возможным решениям (в данном случае – возможным ключам шифрования) присваивается некоторая оценка, а затем выполняется поиск, чтобы найти среди них оптимальную. Решение с наилучшей оценкой, скорее всего, и окажется верным, то есть искомым ключом, используемым для шифрования букв алфавита.

Одним из простых подходов к поиску оптимального решения является тестирование всех возможных решений, то есть поиск методом перебора, но это непрактично, если вариантов для проверки, как в случае использования омофонического шифра, слишком много[39].

Более эффективен, по сравнению с методом грубой силы, стохастический поиск, включающий в себя семейство широко используемых методов. Например, «восхождение на холм» (*Hillclimbing*) – простой и часто используемый метод стохастического поиска. Для оценки возможных решений здесь производится сопоставление омофонов с буквами алфавита: шифртекст сначала расшифровывается с использованием произвольного ключа-кандидата, а оценка, измеряющая качество полученного открытого текста, вычисляется по нижеследующему алгоритму.

- Перед началом поиска вычисляется F_g – относительная частота употребления каждой комбинации из пяти последовательных букв алфавита, называемой *5-gram* или пентаграммой, таких как ISION, EMENT, ETLES, OURLE. Основой для выделения таких пентаграмм служит базовый массив текстов на языке (после удаления в нем пробелов и знаков препинания), на котором, как предполагается, написан открытый текст зашифрованных документов[40].
- Во время поиска с использованием ключа-кандидата оценивается предварительная расшифровка:
  - подсчитывается N_g – встречаемость каждой пентаграммы g в расшифрованном тексте;
  - подсчитывается N_c – встречаемость каждой буквы c в расшифрованном тексте;
  - сумма баллов за предварительную расшифровку S вычисляется по следующей формуле:

$$S = \sum_g N_g \log F_g \Big/ \sum_c N_c^2.$$

[36] *Жак Нау, написавший постскриптумы к нескольким зашифрованным письмам, Гилберт Керлл, о котором известно, что он несколько раз зашифровывал письма Марии [8], а также писал постскриптумы к некоторым из них, и Джером Паскье, который после своего ареста сознался в зашифровывании ее писем (CSP Scotland v. 9, 89, № 80), являются очевидными кандидатами на эту роль, но мы не смогли прийти к какому-либо окончательному выводу.*

[37] *Письмо Кастельно Марии, см. раздел 6.4.*

[38] *В письмах упоминается более ста имен.*

[39] *Точное количественное определение числа возможных ключей для омофонического шифра выходит за рамки данной статьи. Но для сравнения скажем, что количество возможных ключей для моноалфавитного шифра с 26 буквами алфавита равно $26! \approx 4 \times 10^{26}$. В этом случае поиск ключа методом перебора не под силу всем компьютерам мира, вместе взятым. Число возможных ключей для омофонических шифров значительно превышает указанное выше.*

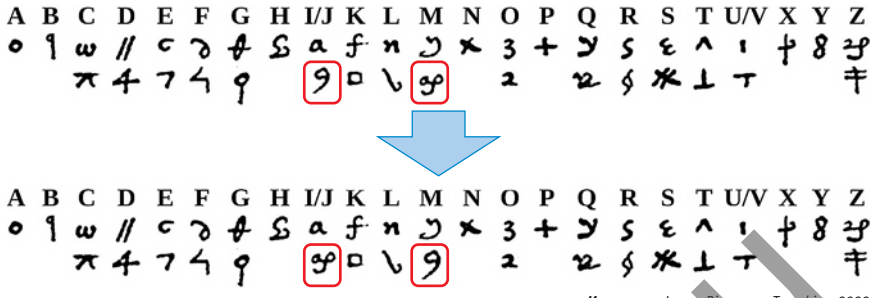
[40] *Для этой цели послужили несколько французских текстов XVI и XVII веков из проекта «Гутенберг». (Проект «Гутенберг» – некоммерческая инициатива, направленная на оцифровку и архивирование произведений культуры, находящихся в общественном достоянии. – Примеч. ред.).*

«Восхождение на холм» начинается с генерации случайного ключа, то есть со случайного сопоставления омофонов буквам алфавита. По ходу «восхождения» итеративно выполняются небольшие изменения в ключе с последующим дешифрованием шифртекста с помощью измененного ключа. Каждый полученный в результате этого расшифрованный текст оценивается по приведенному выше алгоритму, и если полученная сумма баллов для нового варианта превышает предыдущую, измененный ключ сохраняется. Если оценка ниже предыдущей, изменение отбрасывается. Существует два типа внесения небольших изменений, выполняемых во время «восхождения на холм»: замена любых двух символов и переназначение любого из символов, как показано на рисунках А18 и А19 соответственно.

Алгоритм продолжает тестировать различные небольшие изменения в ключе до тех пор, пока сохраняется возможность улучшения результатов, то есть до достижения максимального значения. В большинстве задач оптимизации таких максимумов может быть несколько, но только один из них (глобальный максимум) является правильным решением, тогда как все прочие, называемые локальными максимумами, будут неправильными. Чтобы преодолеть проблему «застревания» на локальных максимумах при «восхождении на холм», алгоритм неоднократно перезапускает весь процесс, каждый раз с другой произвольной начальной точкой. Процесс «восхождения на холм» проиллюстрирован на рис. А20.

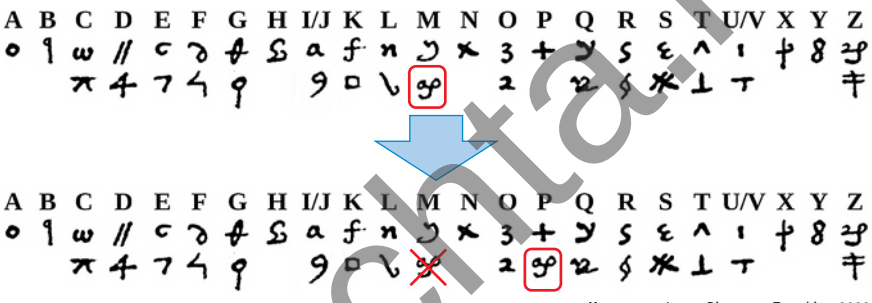
Алгоритм также использует вариацию «восхождения на холм», называемую имитацией отжига, которая решает проблему «застревания» на локальных максимумах, допуская некоторые изменения-«спуски», приводящие к временному ухудшению результата, как показано на рис. А21.

Алгоритм взлома кода восстанавливает только значения омофонов, представляющих собой буквы алфавита. Номенклаторные символы, обозначающие целые слова, части слов, имена или географические названия, необходимо восстанавливать вручную.



Источник: Lasry, Biermann, Tomokiyo, 2022

Рис. А18. ***Замена двух омофонов***



Источник: Lasry, Biermann, Tomokiyo, 2022

Рис. А19. ***Переназначение омофона***

Приложение В. Ошибки шифрования и перекрестная контаминация шифров

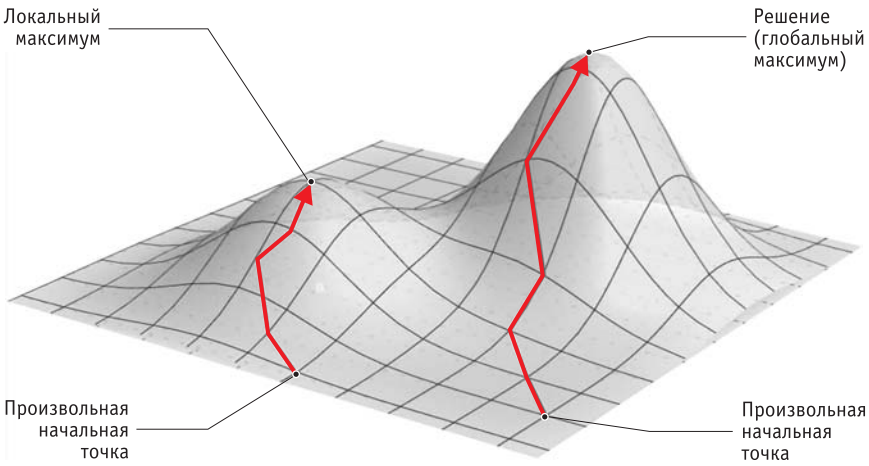
В любом историческом зашифрованном тексте, вероятно, будут возникать случайные ошибки шифрования, такие как пропущенный символ, добавленный дополнительный символ или неправильный символ, используемый вместо правильного. Мы ожидали обнаружить такие спорадические ошибки в наших документах, и в некоторых из них так и произошло. Причем в ряде писем частота ошибок оказалась относительно высокой (до нескольких процентных пунктов), что затрудняло интерпретацию символов и их дешифрование. Более того, углубленное изучение показало, что многие из этих ошибок были систематическими, то есть один и тот же неправильный символ последовательно использовался для шифрования одной и той же буквы алфавита.

Сначала мы рассмотрели ошибки, вызванные визуальным сходством различных шифрсимволов, например, использование символа без точки вместо символа с точкой. Пример подобной ошибки приведен в разделе 4.6. Тем не менее, ошибки такого типа составляют лишь небольшую часть систематических ошибок шифрования.

Изучая другие шифры, которыми пользовалась королева Шотландии, мы заметили, что реконструированный шифр Марии – Кастельно имеет несколько общих черт, таких как диакритические знаки, омофоны и большая часть его номенклатора, с другим омофонным шифром, который мы называем шифром Марии – Битона, использовавшегося узницей для связи с Джеймсом Битоном, архиепископом Глазго и ее послом во Франции[41]. Соответствующая шифровальная таблица показана на рис. В22.

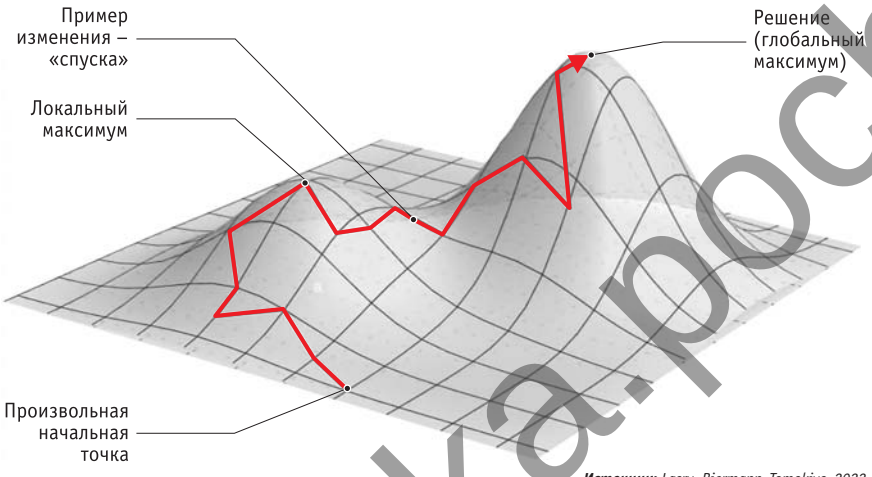
Зная, что письма Марии для Кастельно часто отправлялись вместе с вложениями, адресованными Битону, мы предположили, что систе-

[41] *TNA SP53/23/38. Хотя на шифре стоит дата «1577», он использовался не только в 1577 году, но и в письме Марии Битону от 10 сентября 1582 года, которое с примечанием от Уолсингема Джону Сомеру и датировкой 24 октября 1582 года воспроизведено в [4]. Несмотря на указание в каталоге «вероятно, 1572», его содержание (рейд Рутвена) однозначно соответствует 1582 году.*



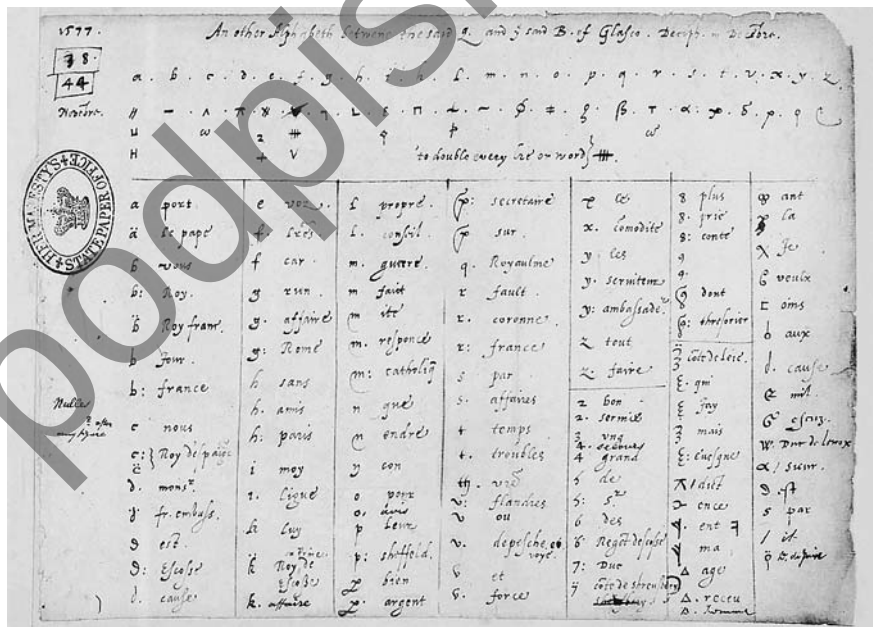
Источник: *Lasry, Biermann, Tomokiyo, 2022*

Рис. A20. ***Восхождение на холм***



Источник: *Lasry, Biermann, Tomokiyo, 2022*

Рис. A21. ***Имитация отжига***



Источник: *TNA SP53/23/38*

Рис. B22. ***Шифр Марии – Битона, 1577 год***

матические ошибки могли возникнуть, когда секретарь зашифровывал несколько писем, используя разные шифры, – явление, которое мы называем перекрестным заражением (контаминацией) шифров. Чтобы проиллюстрировать это явление, на рис. B23 мы показываем количество наиболее распространенных ошибок, обнаруженных в подмножестве из 17 расшифрованных документов. Некоторые из этих ошибок встречаются десятки раз, иногда в пределах одного и того же документа, что подтверждает гипотезу о том, что они носят систематический, а не случайный характер. Некоторые из этих ошибок (выделены на рис. B23) можно объяснить тем, что секретарь ошибочно использовал графический символ, обозначающий нужную букву алфавита (*c*, *i*, *e* и *r*) в шифре Марии – Битона вместо правильного символа из шифра Марии – Кастельно[42]. В других частых и систематических ошибках (таких как первый символ на рис. B23), возможно, были «повинны» другие, неопознанные нами шифры.

Мы сформулировали гипотезу, объясняющую возникновение ошибок перекрестного шифрования при подготовке сразу нескольких писем с применением разных шифров, как это было в случае с рассматриваемыми нами посланиями, которые часто отправлялись с вложениями, адресованными другим получателям.

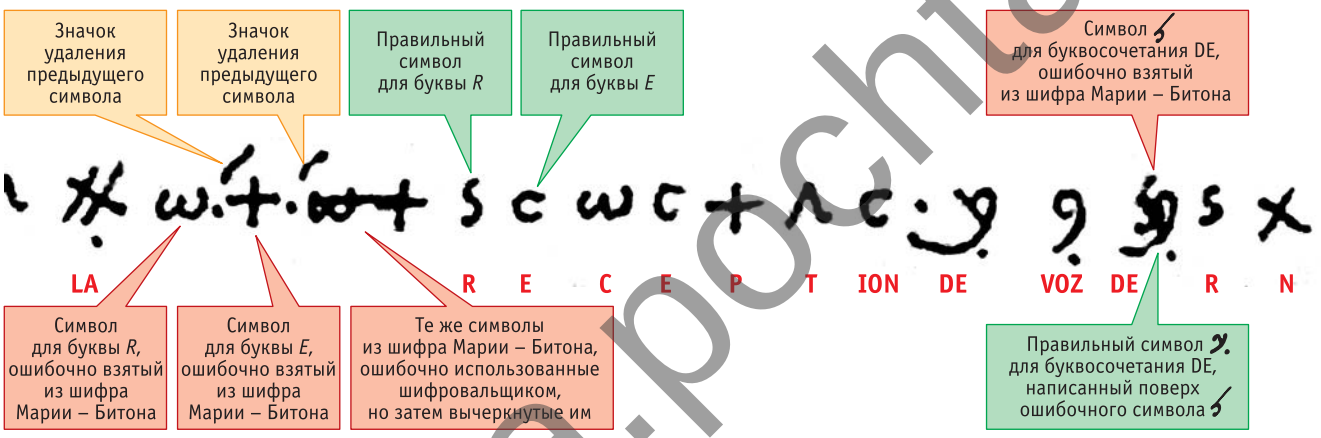
Когда шифровальщик начинает использовать новый шифр, то, вероятнее всего, на первом этапе станет искать правильный графический символ(ы) для каждой буквы алфавита в шифровальной таблице. Но через некоторое время он, наверняка, начнет запоминать символы, которые обозначают наиболее часто встречающиеся буквы алфавита. В отсутствие необходимости постоянно сверяться с таблицей процесс шифрования ускорится. Если тому же секретарю в тот же день нужно зашифровать другое письмо другим шифром, и если для шифрования наиболее часто встречающихся букв алфавита (например, *i* или *e*) он про-

[42] *Символ, соответствующий букве «R» в шифре Марии – Битона, представляет собой незначительную модификацию символа буквы «C» в шифре Марии – Кастельно.*

Предполагаемая правильная буква	Неправильно использованный символ	Значение в шифре Марии – Битона	F307	F105	F109	F118	F123	F125	F130	F30	F34	F50	F54	F64	F74	F82	F87	F89	F98	Всего
I			3		5	20	4			2	4		2	18		3		48		109
C		C	4	1	4	5	3	3				2				5	5			32
I		I	1			3		8	2			2				2	2	2		22
E		E	4			1	1	2	3			3		1		1		2	1	19
R		R						4	1			3						1		9
E								1				2				1		1		5
A											1						4			5

Источник: *Lasry, Biermann, Tomokiyo, 2022*

Рис. B23. ***Повторяющиеся ошибки шифрования***



Источник архивного изображения: *gallica.bnf.fr/BnF fr. 2988 f.26*

Рис. B24. ***Ошибки перекрестного шифрования, исправленные секретарем: вторая строка F26***

должит полагаться на свою память, а не на шифровальную таблицу, он может подсознательно заимствовать символ этой буквы из неправильной шифровальной таблицы, которую он недавно использовал в ходе работы с другим документом. Эта теория также согласуется с систематическим характером таких ошибок: поскольку секретарь не знает о них, он повторяет таковые на протяжении всего документа, с которым он в данный момент работает. Только после того, как мы разобрались в этом интересном феномене, удалось, наконец, расшифровать и правильно интерпретировать многочисленные неясные отрывки в переписке между Марией и Кастельно, обратившись также к значению некоторых символов в шифре Марии – Битона.

Интересно, что в расшифрованных нами документах есть несколько мест, где секретарь смог обнаружить подобные ошибки и исправить их на месте. Он внес эти исправления либо с помощью значка удаления ⁋, либо зачеркнув неправильный символ, либо написав его заново. Интересный пример, иллюстрирующий эти три метода исправления, появляется во второй строке F26 в следующем фрагменте шифртекста: LARECEPTIONDEVOZDERN (рис. B24). Такие исторические исправления являются дополнительным доказательством в пользу гипотезы о перекрестном шифровании. ■

ЛИТЕРАТУРА

1. *Bossy J. Giordano Bruno and the embassy affair // New Haven: Yale University Press. 1991.*
2. *Bossy J. Under the molehill: an Elizabethan spy story // New Haven: Yale University Press. 2001.*
3. *Collinson P. The English captivity of Mary Queen of Scots // Sheffield: Sheffield History Pamphlets. 1987.*
4. *Labanoff A. Lettres, instructions et mémoires de Marie Stuart // Reine d'Écosse: publiés sur les originaux et les manuscrits du state paper office de Londres et des principales archives et bibliothèques de l'Europe. 7 vols. London: Charles Dolman. 1844.*
5. *Leader J. D. Mary Queen of Scots in captivity: a narrative of events from Jan. 1569 to Dec. 1584 whilst Earl of Shrewsbury was the guardian of the Scottish Queen // Sheffield: Leader & Sons; London: George Bell & Sons. 1880.*
6. *Megyesi, B., Esslinger B., Fornés A., Kopal N., Láng B., Lasry G., de Leeuw K., Pettersson E., Wacker A., Waldispühl M. Decryption of historical manuscripts: the DECRYPT project // Cryptologia. 2020. № 44 (6). P. 545–559. – DOI: 10.1080/01611194.2020.1716410.*
7. *Morris J. The letter-books of Sir Amias Poulet, Keeper of Mary, Queen of Scots // London: Burns and Oates. 1874.*
8. *Pollen J. H. Mary Queen of Scots and the Babington Plot // Edinburgh: Edinburgh University Press. 1922.*
9. *Strickland A. Lives of the queens of Scotland. V. 5–7 // Edinburgh: W. Blackwood and Sons. 1854.*
10. *Tomokiyo S. French ciphers during the reign of Charles IX and Henry III, Cryptiana [Электронный ресурс]. – URL: http://cryptiana.web.fc2.com/code/henryiii.htm (режим доступа: 17.11.2022).*
11. *Warnicke R. M. Mary Queen of Scots // Abingdon: Routledge. 2006.*

Информационно-методический журнал

INSIDE
ЗАЩИТА ИНФОРМАЦИИ

Подписная кампания

2024

Единственный в России информационно-методический журнал в области защиты информации
Включен в перечень ВАК при Минобрнауки России

Журнал «Защита информации. Инсайд» решением Высшей аттестационной комиссии включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по следующим научным специальностям:

- методы и системы защиты информации, информационная безопасность (технические науки);
- математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей (технические науки);
- автоматизация и управление технологическими процессами и производствами (технические науки);
- кибербезопасность (естественные науки).

Журнал входит в Российскую систему научного цитирования (РИНЦ).

Оформить подписку на журнал вы можете, заказав ее в интернет-магазине на сайте www.inside-zi.ru, или направив заявку в свободной форме по электронной почте на адрес podpiska@inside-zi.ru, или позвонив по телефону +7 (921) 958-25-50 нашим менеджерам.

Стоимость подписки в редакции

Подписка на полгода (№ 1–3, 2024 г.) – **4224** руб.
Годовая подписка (№ 1–6, 2024 г.) – **8448** руб.

Подписка на электронную версию журнала

Период подписки: весь 2024 год – **7980** руб.
Электронная версия выполнена в формате *.pdf

Специальное предложение: печатная + электронная версии – **10 752** руб. Период подписки: весь 2024 год.

ПОДПИСНЫЕ АГЕНТСТВА:

- **Каталог «Почта России»** (www.pochta.ru)**: ПИ463**
- **ГК «Урал-Пресс»** (www.ural-press.ru)
- **Агентство «Прессинформ»** (presskiosk.ru)
- **Агентство «Книга-Сервис»** (www.akc.ru)

ЭЛЕКТРОННЫЕ АРХИВЫ ПУБЛИКАЦИЙ ЖУРНАЛА за 2015–2023 годы на CD

Полные тексты всех статей с диаграммами, таблицами, графиками, иллюстрациями.

Стоимость с учетом доставки заказной бандеролью – **10 782** руб.

НОВЫЕ ПОСОБИЯ на CD

Практический инструментарий специалиста по защите информации

- Уровни доверия идентификации и аутентификации при удаленном электронном взаимодействии;
- Цифровая криминалистика распределенных реестров;
- Методы и стратегии обороны от DDoS-атак;
- Параметрический выбор криптопримитивов для блокчейн-платформ;
- Квантовая угроза безопасности технологии блокчейн.

Подписной индекс: каталог «Почта России» – **ПИ561**

Ознакомиться с содержанием CD и оформить заказ можно на нашем сайте: www.inside-zi.ru

ООО «Издательский Дом «АФИНА»
194017, Россия, Санкт-Петербург, пр. Тореза, д. 98, корп. 1, офис 315
тел.: +7 (921) 958-25-50, +7 (911) 921-68-24,
e-mail: podpiska@inside-zi.ru,
http://www.inside-zi.ru/

ЛГШ-516Стаф

Генератор шума по цепям электропитания, заземления и ПЭМИ

Предназначен для защиты информации от утечки за счет побочных электромагнитных излучений и наводок путем формирования маскирующих шумоподобных помех.

- Рабочий диапазон частот изделия от 0,009 МГц до 6 ГГц
- Сертификат ФСТЭК России № 4567 от 02.08.2022
- Имеет 5 уровней регулировки выходного сигнала
- Встроенная независимая регулировка уровня шумового сигнала по электрическому и магнитному полям и по сети электропитания и заземления
- Может управляться удаленно — включение/выключение изделия
- Оснащен системой индикации нормального и аварийного режимов работы
- Оснащен счетчиком учета времени наработки в режиме формирования маскирующих помех
- Оснащен энергонезависимой памятью для сохранения настроек изделия

ВАС ПОДСЛУШИВАЮТ? Звоните нам!

СПЕЦИАЛИЗИРОВАННЫЙ ХОЛДИНГ
ЛАБОРАТОРИЯ ППШ

199178, Санкт-Петербург, наб. реки Смоленки, д. 25. Тел: +7 (812) 702-73-83, 309-45-09, 309-61-70
e-mail: lab@pps.ru, www.pps.ru, www.labpps.ru

securika Moscow

29-Я МЕЖДУНАРОДНАЯ ВЫСТАВКА ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ И ОБОРУДОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ПРОТИВОПОЖАРНОЙ ЗАЩИТЫ

16–18 АПРЕЛЯ 2024

МОСКВА, КРОКУС ЭКСПО,
3 ПАВИЛЬОН, 15 ЗАЛ

- ВИДЕО-НАБЛЮДЕНИЕ
- КОНТРОЛЬ ДОСТУПА
- ОХРАНА ПЕРИМЕТРА
- ПРОТИВОПОЖАРНАЯ ЗАЩИТА
- СИГНАЛИЗАЦИЯ И ОПОВЕЩЕНИЕ
- АВТОМАТИЗАЦИЯ ЗДАНИЙ
- ОХРАНА ТРУДА. СРЕДСТВА ИНДИВИДУАЛЬНОЙ ЗАЩИТЫ
- ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

0+

БЕСПЛАТНЫЙ БИЛЕТ ПО ПРОМО-КОДУ: print24

SECURIKA-MOSCOW.RU

ITE ОРГАНИЗАТОР ORGANISER