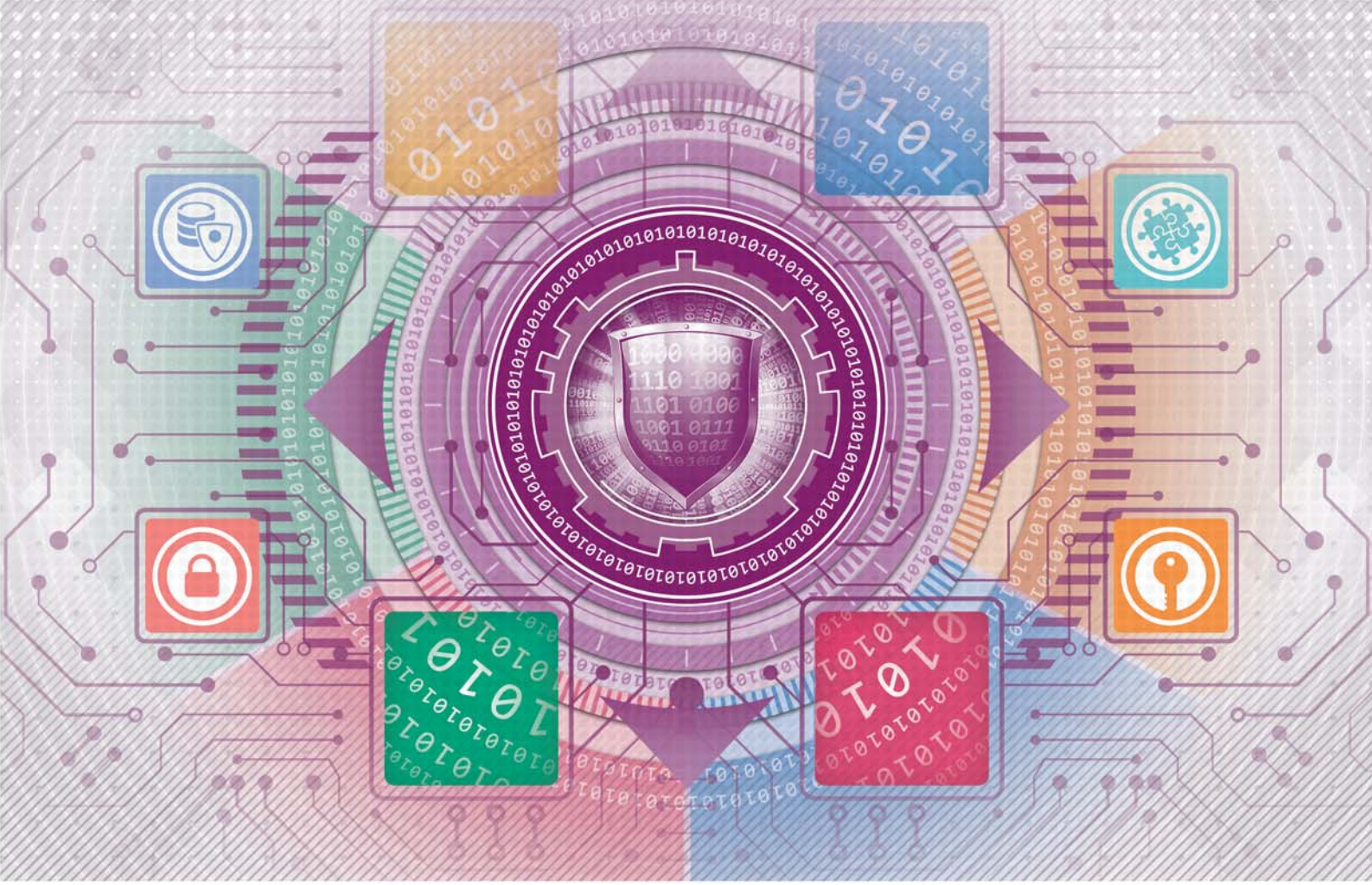
ISSN 2413-3582

Информационно-методический журнал
INSIDE
ЗАЩИТА ИНФОРМАЦИИ
WWW.INSIDE-ZI.RU

№ 6 (108)
2022
ноябрь – декабрь

ПЕРСПЕКТИВНЫЕ РЕШЕНИЯ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ



СПЕЦИАЛИЗИРОВАННЫЙ ХОЛДИНГ
ЛАБОРАТОРИЯ ППШ

АКТУАЛЬНЫЕ МЕТОДИЧЕСКИЕ ПОСОБИЯ

электронная библиотека

Методические пособия из серии «Практический инструментарий специалиста по защите информации»

ООО «Издательский Дом «Афина» и редакция журнала «Защита информации. Инсайд» предлагают вашему вниманию электронные методические пособия из серии «Практический инструментарий специалиста по защите информации».

К разработке пособий были привлечены авторские коллективы ведущих специалистов в области защиты информации, обладающих богатым опытом как практической, так и преподавательской деятельности в рассматриваемых вопросах.

Перечень предлагаемых пособий структурирован по пяти тематическим разделам, представленным ниже:

Общие вопросы обеспечения безопасности информации

- Анализ киберрисков;
- Аудит информационной безопасности;
- Безопасность и устойчивость цифровых экосистем и платформ;
- Инвентаризация и оценка информационных активов;
- Кибернетические и информационные войны;
- Киберустойчивость Индустрии 4.0;
- Мониторинг информационной безопасности;
- Политики информационной безопасности;
- Противодействие экономическому шпионажу;
- Управление киберустойчивостью.

Организационно-правовые вопросы обеспечения безопасности информации

- Безопасность информации в ЕАИС;
- Безопасность АСУТП и КИИ;
- Защита гостайны в РФ;
- Защита конфиденциальной информации;
- Обеспечение безопасности ПДн;
- Организация режима коммерческой тайны;
- Правовое и нормативно-методическое обеспечение специалиста.

Защита информации от утечки по техническим каналам

- Аттестация объекта информатизации;
- Выявление СТС;
- Защита от закладочных устройств;
- Лазерные системы акустической разведки (LSAR);
- Методы и средства защиты информации от LSAR;
- Основы специсследований (ПЭМИН);
- Специалист по технической защите информации;
- Утечка конфиденциальной информации через случайные антенны.

Безопасность компьютерных систем

- Идентификация и аутентификация;
- Национальная система раннего предупреждения о компьютерном нападении;
- Организация доверенной среды облачных вычислений;
- DLP-системы.

Другое

- Кадровая безопасность предприятия;
- Экономическая безопасность предприятия.

Полный перечень и содержание CD – на нашем сайте.

Подписной индекс: ПИ561 (каталог «Почта России»)

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/

Информационно-методический журнал
INSIDE
ЗАЩИТА ИНФОРМАЦИИ

Информационно-методический журнал «ЗАЩИТА ИНФОРМАЦИИ. ИНСАЙД»
№ 6 (108) ноябрь—декабрь 2022 г.
от 01.12.2022

Выходит 6 раз в год.
Очередной № 1'2023 выйдет 02.02.2023

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/

Отпечатано в типографии
ООО «Первый ИПХ»
СПб, ул. Менделеевская, д. 9
Тираж: 1500 экз.

СОДЕРЖАНИЕ

СОБЫТИЯ

Создан маркетплейс российского ПО

Минцифры России объявило о запуске маркетплейса российского ПО.

«На портал Russoft.ru собраны отечественные программные продукты, представленные на рынке и включенные в реестр российского ПО. Правообладатели для размещения своих решений на маркетплейсе подают заявки на Госуслугах», – сообщило министерство в своем Telegram-канале .

По данным ведомства, на маркетплейсе уже размещено более тысячи приложений, а на страницах продуктов описаны их основные характеристики: функционал, стоимость, совместимость с операционными системами и зарубежные аналоги, которые может заместить ПО.

В министерстве подчеркнули, что в ближайшее время функционал Russoft.ru расширится: планируется появление рейтинга продуктов и возможность оставлять отзывы.

По мнению замглавы Минцифры Максима Паршина, маркетплейс должен стать реальным инструментом продвижения программного обеспечения на российском, а в перспективе – и зарубежном рынках.

Пятилетка для российского ПО

Вице-премьер Дмитрий Чернышенко утвердил документ, регулирующий переход предприятий на российский софт. Документ под названием «Методические рекомендации по формированию отраслевых планов мероприятий по обеспечению готовности заказчиков к преимущественному использованию российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, на принадлежащих им значимых объектах критической информационной инфраструктуры РФ» предлагает профильным министрам определиться с организационными мероприятиями, составить планы на срок до 2027 года. Кроме того, они должны заложить целевые показатели эффективности, назначить конкретные сроки перехода на отечественное ПО, персонально определить ответственных.

Как отмечается в документе, для синхронизации заказчиков и исполнителей появятся два перечня:

- организаций, являющихся заказчиками и определяющих совокупность/отрасль/сегмент экономики;
- организаций, являющихся заказчиками и имеющих значимые объекты критической инфраструктуры.

В рамках рабочих групп должны быть выявлены факторы, препятствующие переходу на отечественное ПО и определены функциональные и технологические критерии ко всем классам/типам ПО.

В случае отсутствия необходимого ПО на российском рынке необходимо сформулировать, на какой срок и каким ПО из недружественных стран можно обеспечить решение текущих задач до момента появления отечественной альтернативы. В этом случае, от заказчиков потребуется сформировать четкие требования по тому, какой именно продукт и с какими характеристиками им необходим. Будут сформированы и графики внедрения.

В рекомендациях сказано, что доля отечественного ПО на значимых объектах КИИ должна увеличиться к концу года на 10 % по сравнению с показателями августа. К концу 2023 года она должна превысить первоначальные показатели на 40 %, а в течение 2024–2027 годов все ПО предполагается сделать отечественным.

В МВД создано подразделение по борьбе с киберпреступлениями

В МВД России создали специальное управление по борьбе с преступным использованием ИКТ. Создание структуры обусловлено большим количеством компьютерных атак, дистанционных хищений денежных средств, активным развитием противоправной цифровой индустрии. Соответствующие изменения в структуру ведомства внесены указом Президента России В. В. Путина.

Сотрудники Управления будут бороться с преступлениями, совершаемыми в сфере ИТ-технологий, а также с запрещенным на территории РФ контентом. «Министр внутренних дел РФ Владимир Колокольцев поручил профильным подразделениям ведомства незамедлительно приступить к реализации Указа Президента. Формирование УБК МВД России будет осуществляться за счет перераспределения штатной численности органов внутренних дел и не потребует выделения дополнительного финансирования», – цитирует «Интерфакс» заявление представителя ведомства.

Сегодня каждое четвертое преступление совершается с помощью IT, напоминают в министерстве, поэтому необходима системная работа по борьбе с ними и структура, отвечающая за эту работу.

ЦБ обязал банки ввести идентификацию гаджетов клиентов

С 1 октября вступило в силу указание Центробанка об обязательной идентификации российскими кредитными организациями всех устройств, с которых граждане совершают финансовые онлайн-операции.

Соответствующие требования описаны в указании ЦБ РФ от 18.02.22 № 6071-У, которое вносит изменения в положение Банка России № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

Принятая мера необходима для защиты россиян от кибермошенников. Теперь даже если преступники выманят пароли и коды для доступа в Интернет или мобильный банк, им не удастся войти в личный кабинет жертвы со своего гаджета. Как только банк заметит подмену, он свяжется с клиентом и уточнит, заходит ли тот с другого устройства.

ПЛАНЫ

Минпромторг выступил за отказ от иностранных мессенджеров

Минпромторг РФ направил руководителями промышленных предприятий обращение с просьбой отказаться от использования иностранных мес-

сенджеров и систем видеоконференцсвязи для служебных целей, пишет «Коммерсантъ» со ссылкой на письмо министерства. Как следует из письма, «эта мера необходима для обеспечения безопасности информации, не составляющей гостайну».

Для обеспечения кибербезопасности министерство предлагает прекратить использование в работе как на компьютерах, так и на смартфонах таких популярных мессенджеров и систем ВКС, как Zoom, Skype и WhatsApp. В качестве альтернативы ведомство рекомендует сервисы российских разработчиков, состоящих в реестре отечественного ПО.

Среди мессенджеров и программ видеосвязи, включенных в реестр, – «Яндекс.Мессенджер» и «Яндекс.Телемост», Jazz (разработан «Сбером»), TrueConf, «Контур.Толк», ICQ и «ТамТам», а также «VK мессенджер» (представлен в реестре в составе решений «ВК Экосистема»).

Эксперты считают, что технических проблем с переходом на российские решения не будет, однако может помешать человеческий фактор.

Планируется создание Национального центра по цифровой криптографии...

Минцифры России прорабатывает проект создания Национального технологического центра по цифровой криптографии. Об этом сообщил замглавы министерства Александр Шойтов, выступая на конференции «Пространство безопасности».

Замглавы добавил, что о своем желании работать в рамках центра уже заявили компании «Код безопасности», «Инфотекс» и «КриптоПро». По словам представителя ведомства, в создании центра также примет участие государство. Министерство надеется, что «соответствующая структура будет создана, и она будет обеспечивать частно-государственное взаимодействие и развитие технологий».

Создание центра включено в федеральный проект «Информационная безопасность», сообщил Шойтов и уточнил, что завершиться оно может только в 2023 году.

...и Центра биометрических технологий

Президент России Владимир Путин подписал указ от 30 сентября 2022 года № 693 «Об определении организации, обеспечивающей развитие цифровых технологий идентификации и аутентификации» о создании совместного предприятия (СП) АО «Центр биометрических технологий» (ЦБТ).

Учредителями станут «Ростелеком» (49 % акций), Российская Федерация в лице Росимущества (26 % акций) и Банк России (25 % акций).

Согласно плану, ЦБТ будет заниматься разработкой, развитием и распространением цифровых технологий идентификации и аутентификации (в том числе на основе биометрических персональных данных). Также Центр будет создавать и внедрять сервисы подписания и хранения документов. Кроме того, ЦБТ станет оператором ГИС «Единая биометрическая система» и обеспечит сбор, хранение, обработку и проверку биометрических персональных данных с учетом требований, установленных Федеральным законом.

Минцифры планирует повысить уровень кибербезопасности СМИ

Минцифры разрабатывает механизм регулирования кибербезопасности СМИ. Для этого планируется создать реестр значимых СМИ и подготовить для них перечень недопустимых событий в области кибербезопасности, сообщило издание «Коммерсантъ».

На СМИ не будут распространяться требования законодательства о критической информационной инфраструктуре (КИИ), однако они будут обязаны проводить регулярные проверки защищенности сетей. Также будут разработаны стандарты безопасности для каждого вида СМИ: телевидения, радио и интернет-порталов.

Директор по операционной деятельности РБК Тимофей Щербаков считает, что инициатива крайне полезная, если она позволит создать равномерный уровень кибербезопасности для всей экосистемы СМИ. В других СМИ комментировать инициативу Минцифры не стали.

Представители рынка электроники призывают обновить системы шифрования ТВ-сигнала, заменив их на российские разработки

Несмотря на усилившиеся риски потерять контроль над работой ТВ-сигнала, отечественная телевизионная индустрия по-прежнему использует иностранный софт и оборудование, в том числе и системы шифрования. В России уже сформирован достаточно развитый рынок CAS и DRM, способный предложить операторам свои разработки, однако сила инерции вынуждает последних работать в прежнем ключе. По мнению отечественных разработчиков, это может привести к очень неприятным сюрпризам и тяжелым последствиям.

Данное ПО применяется для защиты ТВ-сигнала от несанкционированного доступа. Операторы устанавливают на передающей стороне технологии шифрования: CAS (*Conditional Access System*) на сетях спутникового, эфирного и кабельного ТВ и DRM (*Digital Rights Management*) в случае интернет-вещания.

Вопрос постоянно обсуждается в ряде Индустриальных центров компетенций, созданных в этом году для оценки возможностей импортозамещения в сфере ПО. Депутат Госдумы Антон Горелкин считает, что детали перехода на отечественные системы кодирования целесообразно определять отдельным нормативным актом – постановлением Правительства РФ, в котором будет подробно прописано взаимодействие участников цепочки по передаче сигнала (вещатели, операторы связи, владельцы аудиовизуальных сервисов, потребители и т. п.), а также сроки выполнения соответствующих мероприятий.

Ренат Лашин, исполнительный директор Ассоциации разработчиков программных продуктов (АРПП) «Отечественный софт», считает, что российским ТВ-операторам на первом этапе достаточно установить отечественные CAS/DRM параллельно с импортными, чтобы избежать полной замены парка приемного оборудования. А вот регистрация новых абонентов должна проводиться уже с помощью отечественных CAS/DRM.

В нынешних условиях, считают эксперты, по-прежнему использовать иностранные технологии в этой сфере не только неоправданно дорого, но и рискованно из-за вполне возможного удаленного отключения или изменения ТВ-сигнала.

Между тем, российские разработки не уступают импортным. Некоторые из них успешно используются крупными отечественными операторами в течение многих лет и успешно проходят регулярный аудит ведущих мировых поставщиков ТВ-контента.

При подготовке новостей использованы материалы сайтов cbr.ru, interfax.ru, t.me/mintsifry, publication.pravo.gov.ru, kommersant.ru и securitylab.ru.

Предложения по коррекции стандартизованной терминологии: пересмотр ГОСТ Р 53114-2008

En **Suggestions for Correction of Standardized Terminology: Revising State Standard (GOST R) 53114-2008**

V. G. Dozhdikov,
PhD (Eng.) Senior Researcher
oooradio@mail.ru
Radiostandart-CNIIRES, Ltd.

The current national standard in the field of entity information security does not take into account aspects related to the security of its staff at all, which contradicts the very concept of 'entity'. It is proposed to supplement the specified terminology standard with new provisions, as well as to revise a number of existing ones. The article provides formulations of terms and definitions, mainly related to the information security of staff entity that were not previously reflected in standard, and also suggests correction of some terms already included in it.

Keywords: national standard, entity information security, correction, term, definition

В действующем национальном (государственном) стандарте в области информационной безопасности организации совсем не учитываются аспекты, связанные с безопасностью ее сотрудников, что противоречит самому понятию «организация». Предлагается дополнить указанный терминологический стандарт новыми положениями, а также пересмотреть ряд существующих. В статье приводятся формулировки терминов и определений, преимущественно относящихся к информационной безопасности персонала организаций, не нашедших ранее отражения в ГОСТ, а также предлагается коррекция некоторых уже включенных в него терминов.

Ключевые слова: ГОСТ, стандарт, информационная безопасность организации, коррекция, термин, определение

Владимир Григорьевич Дождиков,
кандидат технических наук, старший научный сотрудник
oooradio@mail.ru
ООО «Фирма «Радиостандарт-ЦНИИРЭС»

Введение

Нарастание интенсивности информационных войн обусловливает необходимость, в теоретическом плане, совершенствования терминологии в различных областях информационной безопасности (ИБ). В частности, это относится к стандартизованной терминологии по ИБ организаций.

Существует довольно важный национальный (государственный) стандарт ГОСТ Р 53114 [1], устанавливающий основные термины по стандартизации в области обеспечения ИБ в организации.

В 2016 году была принята Доктрина информационной безопасности Российской Федерации [2], где изложена система официальных взглядов на обеспечение ИБ РФ в информационной сфере. В частности, в Доктрине даны основные понятия по ИБ, рассмотрены вопросы информационно-психологического воздействия, формирования культуры личной ИБ, включая граждан, трудящихся во всех сферах деятельности на территории РФ, сотрудников различных организаций.

Согласно определению из пункта 3.3.1 ГОСТ Р ИСО 9000 [3], «организация – лицо или группа людей, связанные определенными отношениями, имеющие ответственность, полномочия и выполняющие свои функции для достижения их целей». В более развернутой формулировке это «объединение людей, совместно реализующих программу или цель и действующих на основе определенных правил и процедур» [4]. При этом, анализ содержания ГОСТ Р 53114 показывает, что он, по своей сути, от-

ражает только те аспекты ИБ, которые так или иначе связаны с информационно-техническими объектами (ИТО) организации, и не затрагивает интересы сотрудников, то есть тех самых людей, упоминаемых в приведенных выше определениях. В стандарте об организации «забыли» об ИБ ее сотрудников, включая вопросы психологии, что является недопустимым.

Учитывая важность и актуальность проблемы обеспечения ИБ как ИТО организации, так и информационно-психологической безопасности людей (сотрудников), представляется целесообразным пересмотреть действующую и разработать новую редакцию ГОСТ Р 53114. С формальной точки зрения, это также важно для упорядочивания текста пересматриваемого стандарта, если учитывать содержание рекомендаций [5].

При разработке новой редакции ГОСТ Р помимо уточнения терминологии, касающейся объектов информатизации, необходимо добавить термины и определения по информационно-психологической безопасности сотрудников. При этом целесообразно учитывать характерные источники информации, например, [6–12] и др.

Ниже в виде статей стандарта приводятся формулировки терминов и определений, которыми целесообразно дополнить ГОСТ Р, а также излагаются предложения по доработке имеющих в ГОСТ Р 53114 статей. Заметим, что приводимая ниже нумерация статей неминуемо будет изменена (скорректирована) в случае появления обновленной редакции пересматриваемого стандарта.

Общие понятия

1. ***Информационная безопасность*** (ИБ): состояние защищенности объекта или субъекта защиты от реализации преднамеренных или непреднамеренных угроз их информационной безопасности.

Примечание. Термин «информационная безопасность» не следует путать с термином «безопасность информации» (пункт 2.4.5 по ГОСТ Р 50922 [13]), который относится только к неодушевленным информационно-техническим объектам/средствам, то есть не затрагивает субъекты защиты.

2. ***Информационная безопасность организации*** (ИБ организации): информационная безопасность объекта, представляющая собой состояние защищенности информационно-технических объектов и специальных выделенных помещений организации, а также ее сотрудников, от реализации преднамеренных и непреднамеренных угроз их безопасности в информационном пространстве.

Примечание. Термин «ИБ организации» скорректирован по сравнению с пунктом 3.2.1 ГОСТ Р 53114.

3. ***Безопасность умственного труда:*** свойство интеллектуальной деятельности человека, включая, в том числе, сотрудников организации, отражающее их защищенность от воздействия неблагоприятных факторов в процессе их жизни и умственной трудовой деятельности.

4. ***Информационно-технический объект*** (ИТО): техническое средство или его составная часть, в основу функционирования которых положены принципы радиотехники и/или электроники, предназначенные для формирования, обработки, хранения, передачи или приема (получения) информации.

Примечание. К ИТО относятся электронные вычислительные машины, персональные компьютеры, автоматизированные системы управления и пр.

5. ***Информационная безопасность сотрудника организации*** (ИБ сотрудника организации): состояние ИБ носителя информации в виде личности, работающей в организации и использующей в своей деятельности конфиденциальную иную закрытую информацию.

6. ***Информационно-психологическая безопасность личности*** (ИПБ личности): информационная безопасность субъекта защиты, представляющая собой состояние защищенности психики человека от реализации в ее отношении преднамеренных и непреднамеренных угроз в информационном пространстве, а также обеспечение целостности его как социального субъекта и возможности адекватного поведения и личностного развития в условиях неблагоприятных информационных воздействий.

Примечание. ИПБ личности можно рассматривать как состояние защищенности сознания человека от действия многообразных информационных факторов, препятствующих или затрудняющих формирование и функционирование адекватной информационно-ориентировочной основы социального поведения человека, а также адекватной системы его субъективных отношений к окружающему миру и к самому себе.

7. ***Информационно-психологическая безопасность*** (ИПБ): состояние защищенности субъекта защиты от негативных информационно-психологических воздействий.

8. ***Субъект защиты:*** личность в Российской Федерации, деятельность которой обусловливается национальными интересами и областью информационного пространства, с которой он взаимодействует.

Примечание. В пересматриваемом стандарте субъектами защиты являются сотрудники организации, включая руководителей организации и прикомандированных лиц.

9. ***Информационное пространство:*** совокупность информации, ИТО, информационных систем и сетей связи, информационных и коммуникационных технологий, а также субъектов (сотрудников организации), деятельность которых связана с данными технологиями, обеспечением информационной безопасности и механизмов регулирования возникающих при этом общественных и производственных отношений.

Примечание. Информационное пространство для сотрудника организации определяется не только ИТО, находящимися внутри организации, но и источниками внешних угроз, включая информационно-психологическое и информационно-пропагандистское воздействие.

Термины, относящиеся к угрозам информационной безопасности

10. ***Угроза информационной безопасности организации:*** угроза ин-

формационной безопасности объекту защиты, представляющая собой совокупность условий, действий и факторов, создающих потенциальную или реально существующую опасность нанесения ущерба организации, ее сотрудникам, используемым информационно-техническим средствам и иным объектам информатизации, связанную с утечкой информации и/или с несанкционированными или непреднамеренными воздействиями на нее.

11. ***Информационно-психологическое воздействие:*** реализация угроз информационно-психологической безопасности, направленных на сотрудника организации, в том числе атак на сознание и подсознание как со стороны коллег, так и от внешних средств информационно-психологического воздействия.

Примечание. Информационно-психологические воздействия могут быть реализованы путем специальных психологических операций, мероприятий и акций, проводимых с помощью информации, пропаганды и агитации, подготовленной соответствующим образом и доводимой до субъекта воздействия с помощью различных форм психологического воздействия (печатными средствами, радио- и телевещанием, изобразительными средствами, через непосредственное общение, материальными акциями, через информационные компьютерные сети), а также путем информационных атак, проводимых в ходе информационных войн.

12. ***Угрозы утечки информации в сетях передачи данных:*** угрозы информационной безопасности, возникающие в процессе функционирования сетей передачи данных.

Примечание. Угрозы утечки информации в сетях передачи данных включают в себя:

- прослушивание каналов, то есть запись и последующий анализ всего проходящего потока сообщений;
- умышленное уничтожение или искажение (фальсификация) проходящих по сети сообщений;
- включение в поток ложных сообщений.

13. ***Информационный терроризм:*** использование информационных ресурсов и/или воздействие на них в информационном пространстве в террористических целях, обусловливающих угрозы или насильственные действия против объектов или субъектов защиты.

Примечание. Информационный терроризм может проявляться, в частности, в виде информационных атак, кибертерроризма, телефонного терроризма.

14. ***Кибертерроризм:*** информационная атака на компьютерную информацию, вычислительную систему, аппаратуру передачи данных, иные составляющие информационной инфраструктуры.

15. ***Телефонный терроризм:*** использование телефонной связи в целях осуществления угроз субъекту, обмана, информационного давления, похищения закрытых сведений.

16. ***Информационная атака:*** стремительное воздействие, предпринимаемое с целью нарушения информационной безопасности какого-либо объекта или субъекта.

Примечание. К информационным атакам относятся в том числе компьютерные и сетевые атаки.

17. ***Компьютерная атака (кибератака):*** целенаправленное несанкционированное воздействие на информацию или ресурс информационной системы либо на получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

Примечание. Компьютерная атака проводится против информационных систем и информационно-телекоммуникационных сетей с применением программно-технических средств с целью нарушения безопасности информации в этих системах и сетях.

18. ***Компьютерный инцидент:*** факт нарушения штатного режима функционирования элемента автоматизированной информационной системы организации.

19 ***Сетевая атака:*** компьютерная атака в виде действий с использованием протоколов сетевого/межсетевого/информационного взаимодействия, направленных на получение несанкционированного доступа в операционную среду компьютера или на нарушение функционирования аппаратных или программных средств компьютера.

Примечание. Термин «сетевая атака» скорректирован по сравнению с пунктом 3.3.7 в ГОСТ Р 53114.

20. ***Информационная война (информационное противоборство, информационная борьба, информационный конфликт):*** взаимосвязанная совокупность действий и информационных атак, предпринимаемых с целью затруднить для противостоящей, противоправной стороны сбор, обработку, передачу, хранение и использование информации, а также с целью обеспечения собственной информационной безопасности.

21. ***Непреднамеренное воздействие на информацию:*** ошибка пользователя информационной системы, сбой технических и программных средств информационных систем, а также природное явление или иное нецеленаправленное информации воздействие, связанное с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию информации, блокированию доступа к таковой, а также к утрате, уничтожению или сбою функционирования носителя информации.

22. ***Недекларированные возможности:*** функциональные возможности средств вычислительной техники и программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Примечание. Термин «недекларированные возможности» скорректирован по сравнению с пунктом 3.3.14 в ГОСТ Р 53114.

23. ***Средство несанкционированного воздействия на информационную безопасность организации:*** злоумышленник, техническое или программное средство, предназначенное для нарушения информационной безопасности организации радиопромышленности, в том числе путем перехвата информации.

24. ***Средство перехвата информации:*** техническое средство, обеспечивающее скрытное получение

информации, в том числе с помощью закладочных средств и средств технической разведки противоправной стороны.

25. ***Средство технической разведки:*** совокупность аппаратуры технической разведки и ее носителя, функционально объединенных для добывания разведывательных данных определенного вида.

Термины, относящиеся к менеджменту информационной безопасности организации

26. ***Менеджмент рисков:*** система менеджмента, устраняющая или снижающая вероятность реализации угроз в отношении организации.

27. ***Менеджмент:*** скоординированная деятельность по руководству и управлению организацией, определяющая разработку, практическую реализацию по поддержанию политики охраны здоровья и обеспечения безопасности сотрудников организации.

28. ***Информационное взаимодействие:*** технологический процесс передачи информации от одного субъекта или объекта к другому.

29. ***Защита выделенного помещения:*** проведение комплекса организационно-технических мероприятий по предотвращению утечек секретной или конфиденциальной речевой информации по техническим каналам за пределы помещения, выделенного в организации для циркулирования такой информации.

30. ***Выделенное помещение:*** специальное помещение, предназначенное для регулярного проведения собраний, совещаний, бесед, переговоров и других мероприятий речевого характера по секретным или конфиденциальным вопросам.

31. ***Зона информационной безопасности организации:*** занимаемый организацией участок пространства и/или территории, в пределах которой проводятся мероприятия по защите информации.

32. ***Силы обеспечения информационной безопасности организации:*** подразделения и должностные лица организации, уполномоченные на решение в соответствии с законодательством Российской Федерации и действующими инструкциями задач по обеспечению информационной безопасности.

33. ***Организационно-технические меры обеспечения информационной безопасности организации:*** совокупность действий и мероприятий, направленных на применение организационных мер, программно-аппаратных и инженерно-технических способов защиты конфиденциальной информации и/или информации, содержащей государственную тайну.

34. ***Средства ликвидации последствий компьютерных инцидентов:*** технологии, а также технические, программные, правовые, организационные средства, включая сети и средства связи, средства сбора и анализа информации, предназначенные для восстановления штатного режима функционирования элементов информационной инфраструктуры после компьютерных инцидентов.

35. ***Бизнес-разведка:*** получение информации, необходимой руководству организации для принятия обоснованных управленческих решений.

Примечание. К интересам бизнес-разведки относятся сведения о процессах в экономике, политике, технологии производства, партнерах и конкурентах, тенденциях рынка.

Заключение

Представляется, что в соответствии с вышеизложенным возможен довольно оперативный пересмотр и последующая разработка проекта нового стандарта ГОСТ Р «Обеспечение информационной безопасности организации. Термины и определения». При этом в ходе подготовки данного документа по стандартизации, по-видимому, некоторые примечания можно будет опустить, а содержащуюся в них информацию поместить в Приложение А «Термины и определения общетехнических понятий, необходимых для понимания текста стандарта» и в Приложение Б «Пояснения и примеры к терминам». В эти же приложения к тексту стандарту при необходимости могут быть помещены некоторые из вышеприведенных понятий. Это обеспечит целостность представленного материала и удобство использования стандарта. ■

ЛИТЕРАТУРА

1. *ГОСТ Р 53114–2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.*
2. *Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 года № 646).*
3. *ГОСТ Р ИСО 9000–2015 Системы менеджмента качества. Основные положения и словарь.*
4. *Новый энциклопедический словарь. – М.: Большая Российская энциклопедия: РИПОЛ классик. – 2006. – 1456 с.*
5. *Р 50.1.075–2011 Рекомендации по стандартизации. Разработка стандартов на термины и определения.*
6. *Термины МЧС России [Электронный ресурс]. – URL: https://www.mchs.gov.ru/ministerstvo/o-ministerstve/terminy-mchs-rossii/ (дата обращения: 13.04.2022).*
7. *Информационно-психологическая и когнитивная безопасность. Коллективная монография; [под ред. И. Ф. Кефели, Р. М. Юсупова]. – СПб.: ИД Петрополис». – 2017. – 300 с. [Электронный ресурс]. – URL: https//pureportal.spbu.ru (дата обращения: 13.04.2022).*
8. *Р 107.СКИП.0012.002–2019. Стандарт организации. Организация и безопасность труда. Информационно-психологическая безопасность. Основные положения, термины и определения. – М.: ООО «Фирма «Радиостандарт-ЦНИИРЭС». – 2020. – 46 с.*
9. *ГОСТ Р ИСО/МЭК 27000-2021. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.*
10. *ГОСТ Р 56255–2014 Термины и определения в области обеспечения безопасности жизни и здоровья.*
11. *Дождиков В. Г. О стандартизации понятий по информационно-психологической безопасности. // Защита информации. Инсайд. – 2019. – № 6 (90). – С. 15–19.*
12. *Атаманов Г. А., Афонин В. Б. Информационная система как объект защиты // Защита информации. Инсайд. – 2020. – № 6 (96). – С. 48–53.*
13. *ГОСТ Р 50922–2006 Защита информации. Основные термины и определения.*

Безопасность искусственного интеллекта

En Artificial Intelligence Security

V. A. Artamonov,
PhD (Eng., Grand Doctor), Full Professor, the Full Member of IAIT
artamonov@itzashita.ru

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

A. E. Safonov,
M. Sc. IT
crocus.usa@gmail.com

The International Academy of Information Technologies (IAIT)

The paper considers the security issues of artificial intelligence (AI). The main mechanism for setting AI to solve a specific problem is machine learning (ML). At the same time, ML is a threat and a vulnerability of AI to various kinds of attacks, the landscape of which is constantly expanding. The paper presents the risks of hacking AI systems in a number of key industries and the categories of attacks on machine learning models. Mathematical and structural models of «hacking» AI through ML technologies are presented and practical recommendations for countering such attacks are given.

Keywords: artificial intelligence, machine learning, cyberattacks, threats, vulnerabilities, cyber resilience, frameworks, structural models of organizing attacks, mathematical models of hacking neural networks, AI information security platforms

В статье рассмотрены вопросы безопасности искусственного интеллекта (ИИ) как сущности, являющейся одновременно и средством обеспечения информационной безопасности, и объектом кибератак. Главным механизмом настройки ИИ на решение конкретной задачи является машинное обучение (МО). В то же время, МО выступает угрозой и одновременно уязвимостью ИИ перед различного рода атаками, ландшафт которых постоянно расширяется. В работе приведены риски взлома систем ИИ по ряду ключевых отраслей, категории атак на модели машинного обучения. Представлены математические и структурные модели взлома ИИ через технологии МО и даны практические рекомендации по противостоянию такого рода атакам.

Ключевые слова: искусственный интеллект, машинное обучение, кибератаки, угрозы, уязвимости, киберустойчивость, фреймворки, математические модели взлома нейросетей, структурные модели организации атак, платформы обеспечения информационной безопасности ИИ

Владимир Афанасьевич Артамонов,
доктор технических наук, профессор, академик МАИТ
artamonov@itzashita.ru

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

Александр Евгеньевич Сафонов,
магистр информационных технологий
crocus.usa@gmail.com

Международная академия информационных технологий (МАИТ)

Введение

Один из законов Паркинсона гласит: если один человек что-то создал, другой обязательно постарается это испортить. Едва искусственный интеллект вышел за пределы лабораторий и стал применяться на практике, как его немедленно начали пытаться «сломать» или заставить действовать в интересах злоумышленника.

Средства обмана ИИ-систем также весьма многообразны. Поскольку искусственный интеллект в процессе машинного обучения учится не «пониманию» происходящего, а выдаче правильных ответов, то самоочевидна идея «неправильного обучения». В датасет «подмешиваются» неправильные данные, например, изображения. И «на выходе», еще недавно правильно работавший механизм распознавания, начинает считать портрет Джоконды автопортретом художника-авангардиста Пикассо. Такую подмену, разумеется, трудно реализовать дилетантам. Зато, если она осуществлена, то ее крайне трудно выявить. Во-первых, принимаемые нейросетевой (НС) системой решения в настоящее время невозможно проверить (методы такой проверки только разрабатываются), а во-вторых, поскольку в более-менее сложной ИИ-модели содержатся тысячи параметров, следовательно, провести ее исчерпывающее тестирование весьма проблематично. Теоретически возможна ситуация, когда ИИ-система будет работать правильно во всех случаях, кроме тех, когда получит ключевой сигнал, определенная реакция на который ранее была заложена в нее злоумышленниками.

Впрочем, научиться обманывать конкретную ИИ-систему можно и удаленно, особенно, если известны алгоритмы ее обучения. А они, секретом, как правило, не являются, наиболее популярные рассмотрены нами в работе [1]. В таком случае можно создать аналогичную модель и поэкспериментировать в поисках ее слабого места. И к поиску «пробивных дата-сетов» привлечь, опять же, ИИ-систему. Такое тестирование, разумеется, часто выполняют и сами владельцы ИИ-решений: пресловутая борьба «брони» и «снаряда» переходит на новый уровень.

Риски систем ИИ для использующих их отраслей

Четвертая промышленная революция Индустрия 4.0, предвестником которой является цифровая трансформация (ЦТ), вызвала бурный рост широкого применения ИИ в ключевых отраслях экономики, военного дела и органах государственного управления. Поэтому «взлом» таких систем ИИ может вызвать крайне негативные последствия для этих отраслей.

Давайте перечислим конкретные примеры.

Автоматизированные транспортные средства

Автоматизированные транспортные средства совершили прорыв как в транспортной отрасли, так и в технике в целом. Такие технологии дали людям надежду на то, что человек, наконец, сможет избавиться от сложной системы управления автомобилем, и вся ответственность на дороге ляжет на искусственный интеллект. Среди основных функций автономных транспортных средств есть компьютерные функции вождения, такие как помощь при парковке или круиз-контроль, предупреждение водителей об опасностях, управление тормозным усилием, рулевое управление и пр.

Несмотря на то, что автономный транспорт во многом решает проблему невнимательности водителя на дороге, говорить о его полной безопасности, увы, не приходится. Ниже мы рассмотрим наиболее распространенные риски ИИ для беспилотных автомобилей и других транспортных средств в целом.

Неправильное распознавание дорожных знаков. Злоумышленники могут внедрять вредоносные наклейки на дорожные знаки. Из-за этих наклеек система автопилота может неправильно распознать сообщение знаков, и водители будут дезинформированы о текущем состоянии дороги или ограничениях скорости. Это может привести к дорожно-транспортным происшествиям и серьезным травмам.

Потеря контроля над полосой. Если злоумышленники изменяют дорожную разметку, системы рулевого управления и контроля полосы движения на основе ИИ могут ввести в заблуждение систему автопилота. Беспилотные автомобили непредсказуемо меняют направление движения, что может привести к серьезным аварийным ситуациям.

Неправильное обнаружение объектов на дороге. Преднамеренные отвлекающие факторы, злонамеренно размещенные на дороге, могут повлиять на своевременное обнаружение автопилотом таких объектов, как другие автомобили, пешеходы и животные, что опять же чревато серьезными дорожно-транспортными происшествиями.

Системы на основе ИИ, использующие биометрические данные

Такие системы могут быть обмануты третьей стороной. Например, специалистам по ИБ уже удалось создать генеративно-состязательные сети, способные производить поддельные отпечатки пальцев , которые выглядят убедительно не только для человеческого глаза, но могут обмануть и электронную систему. Полное совпадение подделки с оригиналом отнюдь не обязательно, поскольку многие распространенные системы распознавания отпечатков пальцев сопоставляют лишь фрагмент отпечатка, что обычно упрощает проведение атаки. Аналогичным образом можно подделать и другие системы на основе ИИ, работающие с различными типами биометрических данных. Кроме того, как и в случае с камерами распознавания лиц, некоторые методы атаки направлены на то, чтобы не дать системе распознать физические данные человека с целью принять его за другого.

Технологии автоматизации

В Индустрии 4.0 все процессы контролируются в режиме реального времени и учитывают изменяющиеся внешние условия; более умные машины способны к самоконтролю и самодиагностике. Многие аспекты автоматизации уже активно используются в производственной отрасли, и большую роль в них играют системы ИИ. С помощью интеллектуальных технологий становится проще осуществлять мониторинг, минимизировать время простоя, предвидеть потребности в обслуживании и контролировать производственные процессы.

Само собой разумеется, что внедрение умных технологий всегда связано с увеличением риска атак на них. Компоненты умной системы взаимосвязаны, что способствует быстроте и эффективности рабочих процессов. Однако удаленные датчики и приемники сигналов могут быть обмануты в случае преднамеренной манипуляции с сигналом. Компьютерное зрение на устройстве можно обмануть, если злоумышленники манипулируют изображениями.

Основная опасность атак на автоматизированное производство заключается в возможности злоумышленника свободно перемещаться по всей производственной сети, атакуя лишь один из ее компонентов. Если он захочет провести атаку на умные инструменты компании-производителя, это может повлиять как на работу автоматизированного оборудования, задействованного в производственных процессах, и изменение технологии производства, так и на безопасность самих сотрудников.

Кроме того, все умные системы используют для своего функционирования огромное количество информации, которая может быть украдена злоумышленниками: будь то информация о технологиях производства, персональные данные или информация о самих умных системах и их алгоритмах.

Сфера наблюдения

Подразумевает любой вид мониторинга с целью сбора информации, в основном, из соображений безопасности. Технологии машинного зрения используются в камерах наблюдения, способных распознавать людей, автомобили и другие объекты.

Системы распознавания лиц можно обмануть, если злоумышленник предъявит фото или видео с определенным человеком на целевую камеру: это самый распространенный вид атаки из-за дешевизны и простоты метода.

Умные камеры наблюдения могут «не замечать» нарушителей в результате применения методов антиобнаружения. Эти атаки выполняются с помощью специальных очков, масок и других аксессуаров.

Системы аудионаблюдения могут неправильно классифицировать подозрительные разговоры в случае использования вводящих в заблуждение ключевых слов.

Системы защиты от мошенничества

Системы KYC/AML[1] – это термин, используемый в сфере банковского и валютного регулирования финансовыми учреждениями и букмекерскими конторами, а также другими компаниями, работающими с частными деньгами. Для достижения этих целей широко используются системы ИИ, поскольку они за несколько секунд выполняют проверку документов, чтобы установить личность человека или законность транзакции.

Несмотря на то, что системы KYC и AML направлены на снижение риска различных финансовых нарушений, атаки на связанные с этими системами устройства – далеко не редкость. Наиболее частая цель злоумышленника при этом – попытаться заставить систему распознать одного человека как другого, а также, внедрив в нее с помощью атаки неверную информацию, попытаться скрыть незаконные транзакции, нежелательные данные о бизнесе или его владельцах и т. п. Кроме того, в результате взлома таких систем более чем вероятно получение злоумышленниками доступа к огромному количеству финансовых данных о людях и организациях, с которыми работает умная система.

В случае манипулирования документами автоматические проверки целостности могут утвердить поддельное удостоверение личности.

Злоумышленники уже научились создавать реалистичные синтезированные голоса или модифицировать существующий голос, чтобы обойти методы голосовой аутентификации.

Системы защиты от мошенничества также можно обмануть с помощью скрытых атак уклонения, заставив эти системы ошибочно классифицировать вредоносные действия как безопасные.

Система мониторинга соответствия может пропустить подозрительные электронные письма и сообщения, если злоумышленники применяют передовые методы уклончивого изменения текста.

Концепция умного города

Концепция умного города подразумевает использование различных видов электронных методов сбора данных, а также технологий Интернета вещей (IoT). Смарт-технологии внедряются в городскую инфраструктуру для упрощения управления внутригородскими процессами и обеспечения комфорта самих горожан. В умном городе применение высоких технологий направлено на оптимизацию аспектов городской жизни, таких как функционирование транспортной системы, управление парковочными зонами, экономия использованных ресурсов, упрощение систем оплаты коммунальных услуг и сбора данных о расходах на коммунальные услуги, повышение безопасности граждан. Таким образом, умный город не основан на одном устройстве или системе, а представляет собой многокомпонентную концепцию, которая использует широкий спектр интеллектуальных технологий и устройств, направленных на обеспечение комфорта и простоты городской жизни.

Безопасность жителей напрямую зависит от безопасности и защищенности систем умного города. Атаки на элементы его систем могут быть самыми разнообразными и провоцировать любой инцидент от сбоев в работе платежных систем и кражи конфиденциальных данных, используемых в персональных смарт-картах граждан, до саботажа услуг по вывозу мусора. Перечислим основные области, где возможно наступление серьезных рисков в результате нарушения штатного функционирования системы умного города.

Конфиденциальность данных. Поскольку все основные данные о гражданах используются в электронном формате, любое их изменение может привести к ряду негативных последствий.

Физическая безопасность граждан. Проникновение злоумышленников в автоматизированные системы, управляющие, например, движением транспорта (интеллектуальные светофоры являются критически важными системами, которые позволяют умным городам уменьшать пробки), особенно беспилотного, или опасными производствами, чреваты наступлением тяжелых последствий для горожан.

Обнаружение объектов – умная уличная камера может неправильно идентифицировать объекты в случае преднамеренных отвлекающих факторов.

Распознавание речи и лиц – смарт-устройство может идентифицировать кого-то другого в качестве владельца дома, автомобиля, ID-карты и т. д.

По оценкам футурологов, уже в 2025 году в 34 умных городах по всему миру будут проживать около 10 млн человек. Однако умные города предоставляют хакерам больше целей для атаки. Если противникам удастся проникнуть внутрь сети, они вполне смогут отключить все от систем сиг-

[1] *KYC (Know Your Customer/Client или «Знай своего клиента») – обязательная проверка персональных данных клиента, обычно со стороны финансового института.*
AML (Anti-Money Laundering) – принципы противодействия отмыванию денег, полученных преступным путем, финансированию терроризма и созданию оружия массового уничтожения.

нализации до водоснабжения, и вызвать полный хаос среди населения.

Умный дом

Умный дом – это набор ИИ-технологий, которые можно применять непосредственно дома для повышения уровня комфорта и качества жизни. Так, системы умного дома подразумевают использование подключенных к Интернету устройств, которые способны выполнять действия и выполнять определенные повседневные задачи без вмешательства человека. Домашняя автоматизация – это гибкая система, которая может быть настроена под потребности владельца.

Одной из особенностей умного дома, которая привлекает пользователей, является возможность удаленного управления домашними устройствами: включением и выключением света, отопления и др., а также автоматизация определенных бытовых функций. И если холодильник, оповещающий о нехватке тех или иных продуктов, может показаться излишеством, то информирование владельца о таких серьезных проблемах, как утечка газа или воды, вторжение посторонних лиц – очевидно полезная функция.

Все устройства умного дома можно разделить на три категории: контроллеры, датчики и исполнительные механизмы (приводы). Устройства управления или контроллеры соединяют все элементы системы друг с другом и с внешним миром. Датчики получают информацию о внешних условиях. Приводы являются наиболее многочисленной группой, в которую входят устройства, непосредственно выполняющие команды.

Злоумышленник способен взломать каждый из трех типов этих устройств и, в зависимости от этого, добиться разных результатов. Эффект может заключаться в простой «шалости» бытовых устройств или же привести к более серьезным последствиям. Например, хакер в состоянии отключить датчики, отвечающие за мониторинг и аутентификацию лиц, входящих на территорию дома, и войти в дом, не опасаясь быть узнанным. Кроме того, одним из слабых мест умного дома является то, что все устройства представляют собой взаимосвязанную систему, обычно связанную со счетом общего владельца. Таким образом, взлом одного из устройств чреват доступом к личной информации владельца дома.

В экосистеме IoT существует множество уязвимостей. Как только злоумышленники применяют преднамеренные отвлекающие факторы, умные домашние камеры могут неправильно идентифицировать объекты.

Если злоумышленники используют обманные инструменты, такие как состязательно модифицированные бинты, пластыри или очки, умные устройства признают своим владельцем кого-либо другого.

Неопознанные лазейки безопасности в любом из устройств умного дома влекут за собой разрешение на открытие дверей посторонним, выключение камер или даже блокировку людей в их собственном доме. Кроме того, злоумышленники могут подслушивать целевых владельцев умных домов.

Категории атак на модели машинного обучения

Существуют разные категории атак на модели машинного обучения в зависимости от фактической цели злоумышленника (шпионаж, саботаж, мошенничество) и этапов машинного обучения (обучение и производство), их также можно назвать атаками на алгоритм и атаками на модель соответственно. Это атаки с уклонением, отравлением, троянскими программами, бэкдорами, перепрограммированием и инференс-атаками [2].

Уклонение (состязательные примеры атак)

Уклонение – наиболее распространенная атака на модель машинного обучения, выполняемая во время логического вывода. Это относится к разработке ввода, который кажется нормальным для человека, но ошибочно классифицируется моделями машинного обучения. Типичный пример – изменить некоторые пиксели на картинке перед загрузкой, чтобы система распознавания изображений не смогла классифицировать результат. Фактически, этот пример может обмануть специалистов, «тренирующих» модель МО. Перед выбором правильного метода атаки следует принять во внимание некоторые ограничения: цель, знания и ограничения метода.

Ограничение целей (целевые, нецелевые и универсальные атаки)

Что такое ложноположительное уклонение? Представим себе, что кто-то хочет неправильно классифицировать результаты, скажем, обойти систему контроля доступа, которая отклоняет всех сотрудников, кроме высшего руководства, или просто нужно «завалить» систему неверными прогнозами. Это и есть ложноположительное уклонение.

Целевые атаки сложнее, чем нецелевые, и теперь их полный список будет выглядеть так:

- *снижение уверенности* – мы не меняем класс, но сильно влияем на уверенность;
- *неправильная классификация* – мы меняем класс без какой-либо конкретной цели;
- *целенаправленная неправильная классификация* – мы меняем класс на конкретную цель;
- *неправильная классификация источника/цели* – мы меняем конкретный источник на конкретную цель;
- *универсальная ошибочная классификация* – мы можем изменить любой источник на конкретную цель.

Ограничение знаний (белый ящик, черный ящик, серый ящик)

Как и при любом другом типе атаки, у злоумышленников могут быть различные ограничения в плане знания целевой системы.

Метод черного ящика – злоумышленник может только отправить информацию в систему и получить простой результат о классе.

Методы серого ящика – злоумышленник может знать подробности о наборе данных или типе НС, ее структуре, количестве слоев и т. д.

Методы белого ящика – о сети известно все, включая все веса и все данные, на которых эта сеть обучалась.

Ограничение метода (l–0, l–1, l–2, l–бесконечность – нормы)

Ограничения метода связаны с изменениями, которые выполняются с исходными данными. Например, если речь идет о распознавании изображений, можно изменить меньше пикселей или наоборот изменить как можно больше пикселей, или выбрать что-то среднее.

На самом деле атаки, основанные на норме *l*-бесконечности (максимальной разнице пикселей), более часты и проще в исполнении. Однако они менее применимы к реальной жизни, так как небольшие изменения могут быть компенсированы качеством камер. Если у злоумышленников есть изображение и они внесли небольшие возмущения в несколько пикселей, они могут обмануть модель. Если у них есть реальный объект и система, делающая фотографию этого объекта, а затем отправляющая эту фотографию в систему МО, есть большая вероятность, что камера распознает большинство возмущений, и фотография возмущенного враждебного примера больше не будет враждебной. Таким образом, атаки, использующие норму *l*–0 или *l*–1, кажутся более реалистичными и более сложными в исполнении.

Другие ограничения, помимо изображений, могут быть в других типах данных. Для текстовых или двоичных файлов ограничения могут быть гораздо более строгими, поскольку невозможно изменить многие входные функции. Создание вредоносного ПО, которое будет обходить решение для анализа, представляет собой более сложную задачу, поскольку входные функции могут иметь еще меньше вариантов для изменения, так что полученный образец вредоносного ПО будет и обходить алгоритм обнаружения, и выполнять свои функции.

Отравление модели МО

Отравление считается одной из самых распространенных атак и может быть разным, как и уклонение. Прежде всего, цели могут быть разными (целевые и нецелевые атаки). Следующее отличие – это ограничение среды, проще говоря, что именно можно сделать для проведения атаки. Можно вводить любые данные или только их ограниченные типы? Можем ли мы вводить данные и маркировать их, только вводить или только маркировать существующие данные?

Существует четыре общих стратегии атаки отравления для изменения модели на основе возможностей злоумышленника.

1. *Модификация меток:* эти атаки позволяют злоумышленнику изменять только метки в наборах данных контролируемого обучения, но для произвольных точек данных. Как правило, с учетом ограничения на общую стоимость модификации.

2. *Внедрение данных:* злоумышленник не имеет никакого доступа к обучающим данным, а также к алгоритму обучения, но имеет возможность добавлять новые данные в обучающий набор. Можно повредить целевую модель, вставив состязательные образцы в набор обучающих данных.

3. *Модификация данных:* злоумышленник не имеет доступа к алгоритму обучения, но имеет полный доступ к обучающим данным. Обучающие данные могут быть отравлены напрямую путем изменения данных перед их использованием для обучения целевой модели.

4. *Логическое искажение:* злоумышленник имеет возможность вмешиваться в алгоритм обучения. Эти атаки называются повреждением логики.

Троянские атаки

При отравлении злоумышленники не имеют доступа к модели и исходному набору данных, они могут только добавлять новые данные в существующий набор данных или модифицировать его. Что касается троянских атак, то злоумышленник попрежнему не имеет доступа к исходному набору данных, но имеет доступ к модели и ее параметрам и может переобучить эту модель. Когда это может произойти? В настоящее время большинство компаний не создают свои собственные модели с нуля, а переобучают существующие. Например, если необходимо создать модель для обнаружения онкологической патологии, они берут самую последнюю модель распознавания изображений и переобучают ее на наборе данных, так как отсутствие данных и изображений рака не позволяют обучить сложную модель с нуля. Это означает, что большинство ИИ-компаний загружают популярные модели из Интернета, где хакеры могут заменить их своими модифицированными версиями.

Идея троянской программы состоит в том, чтобы найти способы изменить поведение модели в некоторых обстоятельствах таким образом, чтобы существующее поведение оставалось неизменным. Как переобучить систему после ввода любых данных, чтобы она все еще выполняла исходную задачу? Исследователи нашли способ: вычтя набор данных из модели, а затем объединив его с новыми входными данными, переобучить модель. Алгоритм атаки трояна представлен на рис. 1.

Бэкдор-атаки[2]

Модификация поведения модели, такая как отравление и троянство, возможна даже в среде черного и серого ящиков, а также в режиме полного белого ящика с доступом к модели и набору данных. Тем не менее, главная цель – не просто внедрить какое-то дополнительное поведение модели, а сделать это так, чтобы закладка (бэкдор) работала и после переобучения системы.

Атака может произойти глобально на основе трех основных принципов.

1. Сверточные НС для распознавания изображений представляют

[2] *Бэкдор, тайный вход (от англ. back door – «черный ход», буквально – «задняя дверь») – дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом.*

собой большие структуры, состоящие из миллионов нейронов. Чтобы внести небольшие изменения в этот механизм, необходимо модифицировать небольшой набор нейронов.

2. Операционные модели НС, способных распознавать изображения, такие как Inception или ResNet, сложны. Их обучают на огромных объемах данных и вычислительных мощностях, которые малым и средним компаниям практически невозможно воссоздать. Вот почему многие компании, обрабатывающие такие изображения, как магниторезонансная терапия (МРТ) или снимки онкологической патологии, повторно используют предварительно обученные НС крупных компаний. Поэтому сеть, изначально нацеленная, например, на распознавание лиц знаменитостей, начинает выявлять раковые опухоли.

3. Злоумышленники могут взломать сервер, на котором хранятся общедоступные модели, и загрузить собственную модель с бэкдором, а модели НС сохранят бэкдор, сделанный хакерами после переобучения модели. Например, исследователи из Нью-Йоркского университета продемонстрировали, что бэкдоры, встроенные в их детектор дорожных знаков, оставались активными даже после того, как они переобучили систему распознавать шведские дорожные знаки вместо американских (рис. 2). На практике обнаружить эти бэкдоры вряд ли возможно, если вы не являетесь экспертом. Но, тем не менее, не так давно вышеупомянутые исследователи предложили решение этой проблемы [3].

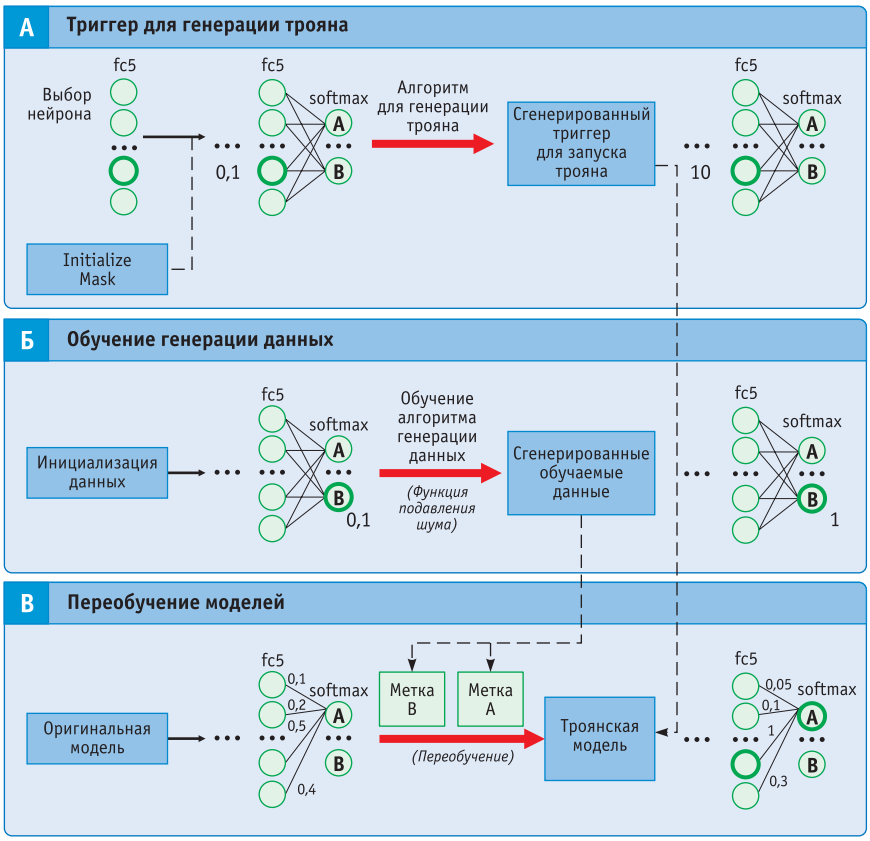


Рис. 1. ***Алгоритм атаки трояна***

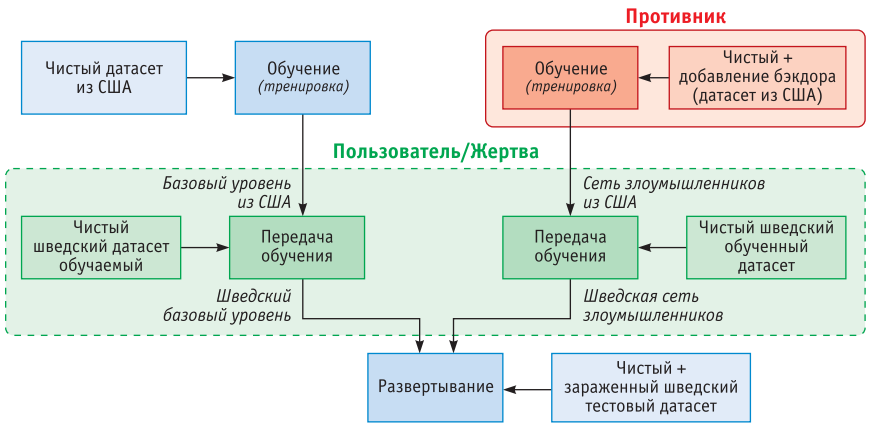


Рис. 2. ***Пример атаки через бэкдор***

Угрозы и уязвимости нейросетей глубокого машинного обучения

Нейросети – перспективная программная парадигма, созданная под влиянием биологии и ИКТ, позволяющая компьютеру учиться на основе наблюдений. НС и глубокое машинное обучение (ГМО)[3] на сегодня дают наилучшее решение многих задач из областей распознавания изображений, голоса и обработки естественного языка. При стандартном подходе к программированию мы сообщаем компьютеру что делать, разбиваем большие задачи на множество малых, точно определяем задачи, которые компьютеру будет легко исполнить. В случае с НС мы, наоборот, не говорим компьютеру, как решать задачу. Он сам обучается этому на основе «наблюдений» за данными, «придумывая» собственное решение поставленной задачи.

Чат-боты[4], распознавание изображений, преобразование речи в текст и автоматические переводы с одного языка на другой – вот лишь некоторые сферы применения НС и ГМО, которое активно вытесняет другие

[3] *Глубокое обучение (глубинное обучение; англ. Deep learning) – совокупность методов машинного обучения (с учителем, с частичным привлечением учителя, без учителя, с подкреплением), основанных на обучении представлениям (англ. feature/representation learning), а не на специализированных алгоритмах под конкретные задачи.*

[4] *Чат-боты на основе ИИ – программы, которые могут в более естественной форме общаться с пользователями. Они используют машинное обучение, обработку естественного языка и анализ настроения.*

подходы. И причина, в основном, в более широких возможностях обобщения при обработке больших объемов данных. А теперь насчет целенаправленных атак. Можно ли использовать особенности работы нейросетей и создать такие псевдоданные, которые будут классифицироваться ошибочно? Рассмотрим несколько способов дополнения данных, которые вводят в заблуждение нейросети глубокого обучения, но при этом для человека данные выглядят неизмененными.

Давайте перейдем к математической модели использования состязательного обучения[5] на примере взлома системы распознавания изображений [4]. Рассмотрим, как искать пиксели изображения, чтобы классификатор принял ошибочное решение.

В основе метода лежит тот факт, что изображения обычно представлены в виде 8-битных значений (каждый пиксель может иметь только одно целочисленное значение в диапазоне от 0 до 255, то есть в сумме 2^8 значений). Следовательно, если искажения не превышают минимального значения, которое может быть представлено в изображении, то классификатор должен полностью их игнорировать и считать искаженное изображение неизмененным. Но это не так.

Ошибочная классификация входных данных определяется уравнением

$$w^T\tilde{x} = w^T x + w^T\eta, \qquad (1)$$

где $\tilde{x}$ – входные данные, предназначенные для введения НС в заблуждение;

$w^T x$ – выходные данные классификатора по неизмененному изображению (которое классифицируется корректно);

η – специальный вектор, добавленный к исходным входным данным таким образом, чтобы вся сеть приняла ошибочное решение о классификации.

То есть уравнение читается так: *«Сеть может ошибиться в классификации, если к оригинальным входным данным добавлены такие данные, что получившийся результат заставляет нейросеть отнести его к другому классу».*

η определяется как:

$$sign(\nabla_x J(\Theta, x, y)), \qquad (2)$$

где *sign*() – знаковая функция (sign function), отвечающая лишь за знак значения (если значение положительное, функция равна 1, если отрицательное – то минус 1);

∇_x – градиенты (относящиеся к входным данным);

J – функция стоимости (cost function), используемая для обучения НС;

Θ – параметры модели;

x – входные данные;

y – целевые выходные данные, то есть «ошибочный» класс.

Поскольку вся сеть является дифференцируемой, значения градиента можно легко найти с помощью метода обратного распространения ошибки (backprop).

Таким образом, изменив входные данные и выяснив с помощью анализа, какое направление нужно изменить (применив информацию о градиентах), можно легко заставить сеть неправильно классифицировать изображение.

В предыдущем примере для обмана нейросети искались небольшие изменения для целого изображения. Однако изменять все изображение не требуется. Вместо этого достаточно изменить небольшую часть, чтобы получившаяся картинка была ошибочно отнесена к другому классу.

Рассмотрим модель однопиксельной атаки.

Для заданных входных данных x вероятность принадлежности x к классу t равна $fx()$. Задача описывается формулой оптимизации

$$Maximize\, e(x) \cdot fadv(x + e(x)), \qquad (3)$$

где adv – оптимизируемый вредоносный класс (adversarial class);

$e(x)$ – вредоносные данные (adversarial data) (такие же, как в предыдущем примере), которые добавляются к входным данным x.

Однако в данном случае у $e()$ есть ограничение:

$$\|e(x)\|_0 \leqslant d.$$

Эта формула означает, что количество элементов в векторе x должно быть меньше настраиваемого параметра d. $\|_0$ означает нулевую норму (*0th norm*) – количество ненулевых элементов в векторе. Максимальное значение элементов, генерируемых $e()$, ограничено, как и в предыдущем примере.

Следует заметить, что инструментарий обмана нейросетей глубокого МО постоянно совершенствуется, свидетельством этому является методика так называемой «вредоносной заплатки».

Вредоносная заплатка (adversarial patch) – новая и весьма эффективная методика генерирования вредоносных изображений, представленная Google. В предыдущих двух методиках вредоносные данные добавлялись к исходным входным данным. Это означает, что вредоносные данные зависят от самих входных данных. Злоумышленники с помощью вредоносной заплатки подбирают некоторые данные, которые подходят для всех изображений. Термин «заплатка» в данном случае нужно понимать буквально: это изображение меньшего относительно входных изображений размера, которое накладывается поверх входных, чтобы обмануть классификатор.

Оптимизация работает в соответствии с уравнением (см. врезку).

Важно отметить, что применительно к уравнению (4) система обучалась на всех изображениях в дата-сете (ImageNet)[6] на всех возможных преобразованиях. И заплата обманывала классификатор на всех изображениях дата-сета. Это главное отличие данного метода от двух предыдущих. Там нейросеть обучалась на одном изображении, а этот метод позволяет подобрать заплатку, которая работает на большой выборке картинок, причем ее можно легко оптимизировать с помощью метода обратного распространения ошибки.

[5] *Состязательное машинное обучение – изучение атак на алгоритмы машинного обучения и защиты от таких атак.*

[6] *База данных ImageNet (дата-сет) – проект по созданию и сопровождению массивной базы данных аннотированных изображений, предназначенный для отработки и тестирования методов распознавания образов и машинного зрения.*

Следует заметить, что обмануть можно не только модели, классифицирующие изображения, но и модели автоматического распознавания речи. Особенность звуковых данных состоит в том, что с помощью метода обратного распространения ошибки входные данные легко изменить нельзя. Причина в том, что входные данные для звукового классификатора проходят через преобразование, для которого требуется вычислить коэффициенты косинусного преобразования Фурье (*Mel Frequency Cepstral Coefficients*, MFCC)[7], используемые затем в качестве входных данных для модели.

К сожалению, вычисление MFCC не является дифференцируемой функцией, поэтому оптимизировать входные данные с помощью метода обратного распространения ошибки не получится. Вместо этого используется так называемый «генетический алгоритм», когда входные родительские данные модифицируются и в результате получаются дочерние данные. Сохраняются те «потомки», которые лучше обманывают классификатор; они, в свою очередь, тоже модифицируются, и так раз за разом.

Рассмотрев математические модели взлома ИИ на примере нейросетей ГМО, перейдем к практической стороне организации структурного механизма таких действий.

Существуют различные точки зрения на архитектурную модель построения механизма компрометации нейросетей ИИ. На наш взгляд, наиболее адекватный подход, к тому же, соответствующий изложенной выше математической модели, предложен ИСП РАН [5].

На рис. 3 представлена структура механизма атаки на модели НС ГМО. Рассмотрим основные составляющие представленного механизма.

Атаки уклонения:

- неразличимые (Imperceptible) атаки:
  - p – норма отклонения от исходного изображения;
  - $p = \infty$ – разрешается изменять каждый пиксель не более чем на ε;
  - $p = 0$ – разрешается изменять произвольным образом не более определенного количества пикселей (известны атаки путем изменения лишь одного пикселя);
- атаки белого ящика – нарушителю доступна полная информация о модели машинного обучения;
- атаки черного ящика – нарушителю доступны только предсказания модели на произвольных входных данных (метки либо вероятности классов);
- универсальные атаки (могут переноситься на другие модели);
- методы защиты в сценариях белого ящика рассматриваются адаптивными процедурами.

Кража данных и моделей из облачных сред:

- формирование цепочек запросов к модели (сценарий черного ящика);
- использование ответов модели как обучающих данных для собственной модели-заместителя (Surrogate Model);
- применение активного обучения (запросы наиболее «сложных» примеров, расположенных близко к границе классов согласно распределению данных);
- развитие методов защиты от кражи моделей (обнаружение подозрительных цепочек запросов, в том числе активного обучения);
- кража моделей (Model Extraction);
- кража данных;
- конфиденциальные данные как результат генерации ответа моделью;
- атака определения принадлежности обучающей выборке (Membership Inference).

Уязвимости в исходном коде фреймворков МО:

- фреймворк машинного обучения TensorFlow, например, содержит

Врезка

$$\hat{P} = arg\ max_p E_{x\sim X,\ t\sim T,\ l\sim L}[\log Pr(\hat{y}|A(p, x, l, t))], \quad (4)$$

где P – подобранная заплатка;
y – целевой (то есть ошибочный) класс;
$A(p, x, l, t)$ – функция применения заплатки, по сути, просто случайным образом решающая, куда и как накладывать заплатку на входное изображение;
p – сам патч;
x – входное изображение;
l – место наложения заплатки;
t – преобразование заплатки (например, масштабирование и вращение).

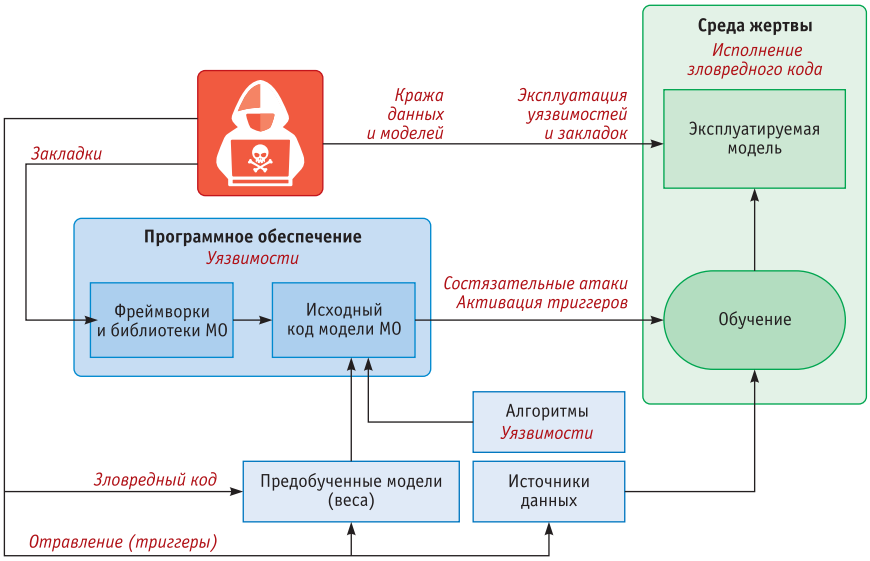


Рис. 3. ***Структура механизма атаки на модели НС ГМО***

[7] *В математике синус- и косинусные преобразования Фурье – формы интегрального преобразования Фурье, в которых не используются комплексные числа. Эти формы предпочтительны в некоторых приложениях, таких как обработка сигналов, речи или статистика.*

около 3 млн строк кода и несколько десятков библиотек зависимостей (Num Py и др.), а классические уязвимости (CVE) в исходном коде фреймворков и библиотек расширяют поверхность атаки на эксплуатируемые модели (примеры: переполнение буфера в библиотеке Open CV, атака с помощью специально подготовленного BMP-изображения);
- в исходном коде возможны закладки (бэкдоры).

Для устранения указанных уязвимостей необходимо провести статический анализ исходного кода фреймворков и создать их доверенные версии.

Встраивание зловредного кода в модели МО:
- встраивание зловредного кода размером до нескольких мегабайт в вещественные параметры (веса) нейросетевых моделей без существенной потери их точности;
- зловредный код не обнаруживается антивирусным ПО;
- компрометация устройства жертвы при использовании предобученных моделей с зловредным кодом, распространяемых через Интернет (GitHub[8] и другие ресурсы).

Отравление данных и моделей МО:
- в небольшое количество обучающих примеров добавляется триггер – специально подготовленный фрагмент изображения;
- обучение на отравленном наборе данных ведет к получению отравленной модели;
- триггер приводит к заведомо ошибочному предсказанию модели на этапе эксплуатации (в том числе к предсказанию заведомо известного нарушителю результата);
- предобученные отравленные модели могут распространяться через Интернет и представлять угрозу при переносе знаний (Transfer Learning).

Многоуровневость и многообразие угроз, специфичных для ИИ:
- угрозы возникают на разных уровнях:
  - уязвимости и закладки в фреймворках машинного обучения;
  - отравление и потеря конфиденциальности данных;
  - алгоритмы (неустойчивость нейросетевых моделей);
- с некоторыми угрозами (отравление) требуется бороться сразу на нескольких этапах жизненного цикла ИИ-систем;
- в разных прикладных ИИ-системах угрозы отличаются, и их количество возрастает;
- требуется комплексное решение.

Платформа и методология создания доверенных ИИ-систем включает в себя:
- модели угроз (нарушителя);
- критерии и методики оценки доверия (бенчмарки[9]);
- программный инструментарий для выявления и противодействия угрозам ИИ;
- доверенные фреймворки МО;
- доступ к среде функционирования, моделям и наборам данных;
- формирование требований к устойчивости к атакам уклонения, отравления и извлечения информации;
- методы противодействия к кибератакам на модели машинного обучения с помощью «объяснения» результатов таких вторжений;
- оценку киберустойчивости вновь разработанных ИИ-систем к атакам на их модели МО;
- механизм обнаружения атак и аномалий в данных, мониторинг дообучаемых моделей МО.

Заключение

Искусственный иетеллект и нейросети используются уже довольно широко. Чат-боты, распознавание изображений, криптология, криминалистика, системы обеспечения ИБ, преобразование речи в текст и автоматические переводы с одного языка на другой – вот лишь некоторые сферы применения глубокого машинного обучения, которое активно вытесняет другие подходы. И причина тому заключается в основном в более широких возможностях обобщения при обработке больших объемов данных (Big Data) с использованием фреймворков.

Возникает вопрос: можно ли использовать особенности работы НС и создать такие данные, которые будут классифицироваться ошибочно? В этой статье мы рассмотрели несколько способов дополнения данных, которые «сводят с ума» нейросети глубокого обучения. И что еще интереснее, эти данные для человека выглядят неизмененными.

Глубокое обучение – превосходный инструмент, который будет использоваться все шире. Изучение способов «обмана» НС, заставляющих их неверно классифицировать данные, позволяет оценить границы предположительного обмана подобных систем и найти способы защиты.

В течение долгого времени разрабатывались специальные типы изображений, известных, как «состязательные», которые сбивают с толку «глаза» ИИ. Используя слабые места в принципах компьютерного «взгляда» на мир, состязательные изображения заставляют машины видеть вещи, которых нет. Их можно рассматривать как вид оптических иллюзий, но предназначенных только для ИИ. Их можно превратить в очки, которые обманут системы распознавания лиц, их можно напечатать на физических объектах, превратить в «заплатки» или «наклейки».

В отличие от других враждебных атак, последние не нужно настраивать на основе изображения, которое они пытаются переопределить, и не имеет значения, где они появляются в поле зрения ИИ. Наклейка позволяет злоумышленникам организовать атаку в физическом мире без предварительного знания условий освещения, угла камеры, типа атакуемого классификатора или других элементов в сцене. Таким образом, после создания такого изображения оно может широко распространяться через Интернет, чтобы им могли воспользоваться другие злоумышленники.

Вот почему многие исследователи ИИ обеспокоены тем, как эти методы могут быть использованы злоумышленниками. Представьте себе небольшую заплатку, которая приклеена на

[8] *GitHub – крупнейший web-сервис для хостинга ИТ-проектов и их совместной разработки.*
[9] *Бенчмарк, (англ. benchmark) – эталонный тест оценки доверия системы ИИ.*

обочину автомагистрали, чтобы беспилотный автомобиль «думал», что он видит знак остановки, или наклейку, которая не позволяет системам наблюдения с искусственным интеллектом идентифицировать вашу личность. Даже если люди заметят эти пятна, они не смогут понять их сути, а в лучшем случае воспримут как некие арт-объекты.

Конечно, несмотря на высокую эффективность враждебных изображений, они не являют собой какой-то супермагический прием, который всякий раз срабатывает на каждой системе ИИ. Уже выходят соответствующие патчи, в частности, созданные исследователями Google, но их создание требует времени, а главное, доступа к коду систем машинного зрения, которые они призваны защитить. Проблема заключается также в том, что подобные атаки со временем становятся все более гибкими и эффективными.

Сейчас в области машинного обучения активно развиваются решения и продукты, связанные с генерацией кода (Copilot, AlphaCode и др.). Компании, разрабатывающие такие решения, предоставляют доступ к ним в виде некоторого сервиса или плагина, встроенного в среду разработки. В арсенале подобного рода решений имеется множество инженерных и технологических нюансов, но ключевым элементом (как и для большей части задач машинного обучения) являются данные для обучения/разработки модели. Под моделью здесь имеется в виду непосредственно алгоритм (на базе НС), отвечающий за генерацию кода.

Качество, вариативность и надежность данных, на которых обучается модель, напрямую влияют на то, что клиент/разработчик будет получать от подобного решения на выходе. Чаще всего для сбора данных для обучения используют открытый код (например, GitHub), которого в Интернете в избытке, но никто не застрахован от того, что в этом коде может находиться вредоносная закладка (бэкдор), способная моментально вывести из строя работающий сервис клиента.

Основной целью бэкдора является скрытное и быстрое получение доступа к данным, в большинстве случаев – к зашифрованным и защищенным. Например, бэкдор может быть встроен в алгоритм шифрования для последующего прослушивания защищенного канала злоумышленником.

Основные особенности бэкдора:

- сложно обнаружить;
- можно использовать многократно;
- легко отрицать злой умысел: выглядит как ошибка, и в случае обнаружения разработчик может сослаться на то, что допустил эту ошибку случайно;
- эксплуатируется только тем, кто знает, как активируется бэкдор;
- защищен от компрометации предыдущими использованиями: даже в случае обнаружения невозможно установить, кем бэкдор эксплуатировался до этого и какой информацией завладел злоумышленник;
- сложно повторить: даже если бэкдор был кем-то найден, его невозможно будет использовать в другом коде или в другом устройстве и др.

В идеальном случае, когда все процессы выстроены, при обучении моделей разработчики фильтруют данные для обучения, а клиент/разработчик перед тем, как использовать код, сгенерированный моделью, его анализирует и адаптирует. Далее код проходит несколько шагов тестирования до того, как попадет в сервис. Но это идеальной случай, а так бывает не всегда.

Наконец, не стоит забывать о пресловутом «человеческом факторе» в лице так называемых специалистов в технологиях «интеллектуального анализа данных» (Data Mining) и «науки о данных» (Data Science). Обе эти категории специалистов, обладающих высокими компетенциями в математике, статистике, работе с большими данными, программировании и пр., как правило, не состоят в штате компаний и организаций, использующих системы ИИ в своей производственной деятельности, а являются приглашенными сотрудниками аутсорсинговых компаний, выполняющих работу по обучению и адаптации МО под задачи заказчика. По существующему в большинстве стран законодательству, кроме отдельных статей Уголовного Кодекса, относящихся к общему характеру использования компьютерной техники в осуществлении преступной деятельности, данные лица и компании, ввиду латентности данного вида деятельности, не подпадают под преследование по закону. Из этого следует, что в существующее законодательство необходимо внести дополнения, касающиеся лицензирования деятельности компаний в области ИИ и МО, а специалисты, привлекаемые к этим работам, должны иметь соответствующие сертификаты компетенции и давать подписку (заключать соглашение) о неразглашении сведений об используемых при создании систем с использованием искусственного интеллекта данных и доверенных средств (фреймворков), что особенно важно применительно к критической информационной инфраструктуре и системам военного назначения. Однако это уже другая проблема, которая требует отдельного изучения. ■

ЛИТЕРАТУРА

1. Артамонов В. А., Артамонова Е. В., Сафонов А. Е. Искусственный интеллект: когнитивное начало // Защита информации. Инсайд. – 2022. – № 4 – С. 50–59.

2. Как атаковать машинное обучение // machinelearningmastery.ru. Машинное обучение, нейронные сети, искусственный интеллект [Электронный ресурс]. – URL: https://machinelearningmastery.ru/how-to-attack-machine-learning-evasion-poisoning-inference-trojans-backdoors-a7cb5832595c/ (дата обращения: 23.07.2022).

3. Liu K., Dolan-Gavitt B., Garg S. Fine-Pruning: Defending Against Backdooring Attacks on Deep Neural Networks // New York University, Brooklyn [Электронный ресурс]. – URL: https://arxiv.org/pdf/1805.12185.pdf (дата обращения: 21.07.2022).

4. Четыре способа обмануть нейросеть глубокого обучения // Блог компании Mail.ru Group. [Электронный ресурс]. – URL: https://habr.com/ru/company/vk/blog/348140/ (дата обращения: 23.07.2022).

5. Аветисян А. И. Использование доверенного ПО при создании систем искусственного интеллекта как основа безопасности (доклад) // XXVII научно-практическая конференция «Комплексная защита информации», 24–26 мая 2022 года, Московская область.

Анализ информационной безопасности блокчейн-технологии Hyperledger Fabric

En **Information Security Analysis of Hyperledger Fabric Blockchain Technology**

A. M. Sizov
gipno2009@yandex.ru
Financial University under the Government of Russian Federation

Hyperledger Fabric is one of the most popular private blockchains and has a huge impact on the blockchain industry. However, not many scientific works analyze the risks related to the information security of the Hyperledger Fabric system architecture and consensus protocols. This article will consider possible vulnerabilities of the following system components: Consensus, chaincode, network and privacy. Also, this article will analyze measures to react and prevent the exploitation of these vulnerabilities and keep the Fabric system intact. The purpose of this article is to analyze the threats to the security of the system, as well as to eliminate the vulnerabilities of a potential and strong technology, and, finally, to motivate scientific researchers to conduct further research on the information security of blockchain systems.

Keywords: Hyperledger Fabric, cybersecurity, blockchain, Kafka, Raft, security threats, vulnerabilities

Hyperledger Fabric (HF, Fabric) является одним из самых популярных блокчейнов с доступом и обладает огромным влиянием на блокчейн-индустрию. Однако не так уж и много научных работ анализируют риски, касающиеся информационной безопасности архитектуры указанной системы. В данной статье рассмотрены возможные уязвимости следующих ее механизмов: консенсуса, чейнкода (кода цепочки), сети и конфиденциальности. В частности, проведено сравнение ряда протоколов консенсуса и предложен выбор оптимального для внедрения в Fabric. Рассмотрены такие возможные уязвимости блокчейн-сети как «скомпрометированный поставщик услуг членства» и безопасность процесса идентификации пиров, подтверждающих транзакции. Кроме того, в публикации указаны меры, направленные на противодействие эксплуатации этих уязвимостей и сохранение системы Fabric в целостности. Так, описаны подходы, которые могут быть использованы в будущем для проработки механизмов уменьшения сетевых рисков HF, такие как обеспечение защиты MSP и использование псевдонимов у подтверждающих нод. Рассмотрены вопросы приватного сбора данных и их защищенного хранения в распределенном реестре. Цель статьи заключается в том, чтобы мотивировать научных исследователей к проведению дальнейших изысканий в области информационной безопасности блокчейн-систем, направленных на устранение уязвимостей этой перспективной и потенциально сильной технологии.

Ключевые слова: Hyperledger Fabric, блокчейн, информационная безопасность, Kafka, Raft, угрозы, уязвимости

Алексей Максимович Сизов
gipno2009@yandex.ru
Финансовый университет при Правительстве РФ

1. Введение

В последние несколько лет было создано и предложено пользователям бесчисленное количество блокчейнов с доступом, и практически каждый из них описывался как блокчейн, который знаменует собой переворот в самой концепции технологии, а также гарантирует приватность и информационную безопасность своих внутренних механизмов.

Блокчейн Hyperledger Fabric (он же Fabric или HF) в последнее время был внедрен в сотни различных ИТ-

проектов по всему миру. Данная система привлекает разработчиков своей расширяемостью, отказоустойчивостью и стабильностью работы. Вследствие этих и прочих присущих ей преимуществ можно сказать, что HF на текущий момент является лучшей и наиболее эффективной среди блокчейнов с доступом, которые создаются для внутренних систем организаций. Например, за 2020 год, HF был признан самым используемым распределенным реестром в экосистемах Интернета вещей (IoT) [2], финансировании цепочек питания [3], работы с медицинскими данными [4] и др.

Итак, Fabric является блокчейн-технологией «с доступом», то есть представляет собой закрытую систему, в которой считывать и записывать данные в общий блокчейн (реестр) могут только участники, получившие специальный доступ к системе. Этих участников называют пирами (peers), и только часть из них может одобрять транзакции. Чтобы доказать свое право на подтверждение транзакции, пиру необходимо подтвердить свою личность при помощи электронной подписи [5]. Благодаря данной настройке участникам легче и быстрее работать с транзакциями, и обычно именно это является одной из главных причин, почему Fabric намного быстрее других блокчейнов с доступом.

За идентификацию всех присутствующих в блокчейне нод (nodes, то есть узлов системы – участников, таких как пиры, клиенты, обслуживающие ноды и др.) отвечает специальный «поставщик услуг членства». Он является одним из самых важных аспектов системы HF, так как полностью отвечает за доступ к системе посредством передачи нодам учетных данных в форме криптографических сертификатов, используемых для аутентификации и авторизации.

Еще одной особенностью Fabric является то, что ее возможности не ограничиваются ею самой: есть возможность расширить алгоритмы консенсуса. HF предоставляет очень широкий спектр возможностей расширяемости и конкретизации работы нод, отвечающих за общий порядок построения транзакций. Также, начиная с версии 1.0, в системе Fabric не используется консенсусный алгоритм практической византийской терпимости к ошибкам (*Byzantine Fault Tolerance*, BFT)[1], что потенциально может привести к созданию большого количества злонамеренных нод. В HF поздних версий применяются только протоколы устойчивости от сбоев (*Crash Fault Tolerance*, CFT), которые работают на Kafka или Raft.

Практически во все существующие на сегодняшний день блокчейны с доступом могут быть внедрены смарт-контракты: мини-приложения, которые вызываются каждый раз при предложении транзакции. В случае HF смарт-контракты выполняются при помощи программного кода, написанного на языке Go, так называемого «кода цепочки» или же чейнкода (chaincode). Последний выполняется некоторым количеством пиров на локальном уровне. До того, как каждая транзакция будет присоединена к блокчейну, вывод данного чейнкода учитывается для результата корректности самой транзакции, а также для выбора данных, которые будут включены в сам блокчейн.

Статья построена следующим образом: во второй главе проанализирована научная литература по технологии Hyperledger Fabric. В третьей главе анализу подвергнут механизм консенсуса HF вместе с возможностью введения механизма BFT, который может быть внедрен для усиления защиты от действий злонамеренных нод. В главе 4 анализируются угрозы сети системы (например, какие атаки возможны на систему при нарушении работы поставщика услуг членства), а также предлагаются способы защиты от данных угроз. Глава 5 посвящена завершающему анализу защищенности системы Fabric, а также поднимает остающиеся открытыми вопросы по некоторым из возможных угроз данной системе.

2. Анализ литературы, посвященной технологии Hyperledger Fabric

В 2009 году человеком или группой людей под псевдонимом Сатоши Накамото была разработана первая цифровая валюта (криптовалюта) биткойн, о чем было заявлено посредством так называемой «белой бумаги» (whitepaper) [1], то есть основополагающего документа, который принято выкладывать при появлении новой технологии, содержащего необходимое для понимания ее основ описание. В указанной статье было предложено решение проблемы двойной траты, не прибегая к услугам третьих доверенных лиц. Децентрализованная архитектура биткойна и блокчейна вместе с механизмом консенсуса доказательства работы (*Proof-of-Work*, PoW,) улучшили прозрачность, доверие и проверяемость транзакций. За счет данных преимуществ понятия «биткойн» и «блокчейн» вызвали интерес и заслужили доверие в технологическом и научном сообществе.

Первоначально специфика и идея криптовалюты выглядели очень пер-

[1] *Byzantine fault tolerance – в криптографии – задача взаимодействия нескольких удаленных абонентов, которые получили приказы из одного центра, также называемая задачей консенсуса византийских генералов. Часть абонентов, включая центр, может быть злоумышленниками (или злоумышленники подменили сообщения при передаче). Нужно выработать единую стратегию действий, которая будет выигрышной для абонентов.*

*Исходная формулировка такова. Византийская армия накануне важного сражения состоит из **n** легионов под командованием своего генерала. Также у армии есть главнокомандующий. Между тем, империя в упадке, и любой из генералов и даже главнокомандующий могут оказаться предателями. Ночью все генералы получают от главнокомандующего приказ, как надлежит поступить утром. Возможные варианты приказа: «атаковать» или «отступать». В случае предательства главнокомандующего он мог дать разным генералам противоположные приказы, чтобы обеспечить уничтожение армии по частям. Если каждый генерал примет решение независимо от других, то вероятность благоприятного исхода сражения весьма низка. Поэтому генералы нуждаются в надежном обмене информацией между собой, чтобы прийти к единому решению.*

спективно, особенно в сфере финансов, однако затем стали проявляться проблемы в скриптах технологии. В конце 2014 года Виталиком Бутериным была выпущена «белая бумага», в которой были представлены проблемы биткойна, в результате чего им был представлен абсолютно новый концепт смарт-контрактов [6]. Введение смарт-контрактов в совокупности с существующими преимуществами технологии привлекли внимание владельцев бизнеса и появились предложения о внедрении блокчейна в ИТ-системах организаций, в особенности, логистического направления.

Где имеется интерес, там есть и развитие: в 2015 году на рынке блокчейна появилась новая технология Hyperledger Fabric с «белой бумагой» [7], которая вскоре обогнала своих конкурентов ввиду больших возможностей и меньшего количества ограничений системы. В последнее время в рамках новых технологических решений было создано множество инноваций для достижения большей работоспособности, чему также способствовало появление новых направлений, таких как Интернет вещей, машинное обучение, кибербезопасность и т. д. Теперь мы можем констатировать, что технология HF представляет интерес не только для научных исследований [8–10], но и на практике: организации все чаще и чаще внедряют данную технологию в свои системы для повышения их продуктивности [11, 12].

Многие аспекты информационной безопасности Hyperledger Fabric уже рассматривались ранее, например, в работах [13–16]. Однако технология не стоит на месте и часто обновляется, но наряду с ее совершенствованием приходят и новые уязвимости, и новые угрозы, основные из которых будут рассмотрены в данной статье.

3. Описание системы Fabric и протоколов консенсуса

Поддержка различных встраиваемых протоколов консенсуса является ценным преимуществом блокчейн-систем. Выбор корректного протокола означает формирование корректной модели защиты для конкретного блокчейна [17]. Так, если блокчейн используется в небольшой ИТ-системе, которая поддерживается организацией или доверенной стороной, ввод продвинутых и сложных протоколов можно расценивать как необоснованную трату ресурсов. Поэтому ввод одной мастерноды (*Ordering Service Node,* OSN) для достижения консенсуса и обработки заявок пользователей в небольшой системе с максимальной защищенностью является правильным решением при выборе корректного протокола консенсуса.

Приведем ряд протоколов консенсуса

1. *Solo* – централизованный протокол консенсуса, который вводится для тестирования, так как данному механизму необходима только одна нода для получения и обработки входящих транзакций. Применяя данный подход, разработчик может сфокусироваться на других проблемах, таких как создание и улучшение чейнкода. Однако стоит учитывать, что в Solo присутствует единая точка отказа (SPoF), то есть в случае отказа ноды вся система также перестанет работать.

2. *Apache Kafka* – это распределенный протокол, который используется для передачи большого количества логов (журнала записей) с очень низкой скоростью задержки. В системе Kafka присутствуют четыре главных компонента: создатели, темы, потребители и брокеры. Записываемая в блокчейн информация поступает от создателей в поток сообщений под названием «темы», которые являются партициями (частями) файловых сегментов. Сообщения хранятся у брокеров как самый поздний файловый сегмент, и в момент добавления сообщений в партицированные логи только пользователи с доступом могут обрабатывать данные сообщения при помощи заявок брокерам.

Механизм отказа Kafka исходит из ZooKeeper и работает по принципу копирования партиций между брокерами. У каждой партиции есть свой «лидер», действия которого копируются «подписчиками». Если имеет место сбой у лидера, то начинается процесс выбора нового лидера из подписчиков. Если говорить о показателях эффективности, то Kafka показал хорошие результаты [17] и внес существенные улучшения в область блокчейнов, встроенных в бизнес-процессы. Тем самым можно сказать, что Kafka превзошел Solo и является предпочитаемым протоколом в версии Fabric 1.0.

3. *Raft* – это протокол консенсуса [18], также основанный на концепции «выбора лидера» для организации консенсуса за счет выбора главной ноды, которая получает различные данные от пользователей и копирует их. Для поддержания стабильности системы и корректного выбора лидера протокол разделяется на три фазы: фазу выбора лидера, фазу копирования лога и фазу безопасности. Время в данном протоколе разбивается на периоды, называемые «сроками», и каждый срок является инкрементом предыдущего.

Ноды в Raft имеют иерархическую связь с лидером во главе и подчиненными подписчиками или же кандидатами. Лидер – это важная личность протокола, и она выбирается единой на каждый канал. Его задача – взаимодействовать с клиентами, а затем копировать свои записи для синхронизированных с ним подписчиков. Следовательно, чтобы получить наилучшую степень синхронизации, система отправляет систематические сообщения проверки своим подписчикам, и если возникает хотя бы слабое подозрение, что сеть лидера перестала работать, как минимум, один из подписчиков сможет определить эту проблему, запустить голосование в сеть и попробовать занять место лидера [19]. Некоторые ноды могут соревноваться друг с другом, чтобы выиграть голосование посредством запроса голосов от других нод. Такие ноды называются «кандидатами».

В протоколе Raft присутствует обязательное условие, что только одна нода может стать лидером (даже при пропуске сроков у других нод или разделения блокчейна). В первом случае устаревшая нода поменяет свой срок и станет подписчиком, во втором – текущий срок закончится

без какого-либо выбора в голосовании.

Производительность Raft еще не полностью протестирована, но его внедрение является предпочтительным протоколом консенсуса, начиная с версии 1.4.1, так как было установлено, что этот протокол может обрабатывать тысячи транзакций в реалистичных сценариях [7], а задержка вывода транзакций у него даже меньше, чем в протоколе Kafka.

4. *BFT-SMaRt* – протокол консенсуса, написанный на языке Java, который предлагает защищенные алгоритмы работы для Fabric [21]. При условии отсутствия в системе дубликатов блокчейнов, требующих валидации, BFT-Smart может показывать почти идеальные результаты решения «проблемы византийских генералов». Один из компонентов системы под названием WHEAT [21] обеспечивает эффективную систему распределения голосов, низкий уровень задержки и быстрое копирование среди нод, не нарушая безопасности сети. Сама система состоит из так называемых кластерных нод и фронтендов. При использовании DFT-SMaRt в роли протокола консенсуса системы поток транзакций практически аналогичен обычному потоку транзакции в HF [17]. При одобрении пиров пользователь генерирует подписанный «конверт», который содержит описание канала передачи, а также одобрения пиров вместе с их подписями [17]. Этот «конверт» распространяется по фронтендам и далее отправляет к административным нодам для входа в цепочку. После того как административная нода собирает нужное количество «конвертов» от доверенных фронтендов, или же когда кончается определенное время, создается новый блок в системе, который содержит корректные транзакции. Следовательно, валидация блоков отличается от стандартной генерации [17], и блоки появляются только благодаря подписям подтвердивших их участников. Наконец, блок перемещается к фронтендерам, а затем к пирам, которые администрируют блокчейн. Анализ производительности BFT-SMaRt показывает, что он способен обеспечить пропускную способность в размере более 10 000 транзакций в секунду с временем подтверждения блока менее секунды [21].

Сравним приведенные протоколы консенсуса и выберем оптимальный для внедрения в систему Fabric.

Наличие в Solo единой точки делает протокол непригодным для внедрения в условиях реальных организаций. Raft и Kafka имеют преимущество механизма «лидер – подписчик», чтобы справляться с отказами системы, но в Kafka, несмотря на популярность, необходимо учесть и корректно обработать несколько важных замысловатых компонентов системы (в Raft эти компоненты уже встроены в обрабатывающую службу [7], то есть остается меньше компонентов, подверженных отказам). Предполагается, что блокчейн Kafka станет внедряться в окружение с малым количеством нод, а кластер будет обрабатываться единой сущностью (административной нодой). Данный концепт нельзя назвать полностью децентрализованным, так как, по сути, все пользователи зависят от этой сущности. Raft же наоборот более децентрализован, более расширяем и может показывать намного более высокие показатели пропускной способности [20].

По совокупности указанных причин, можно сказать, что протоколы консенсуса Raft и Kafka уже устарели в версии Fabric 2.0. Однако, несмотря на устаревание Kafka, перестройка потока транзакций Fabric позволила ускорить пропускную способность этого протокола от 3,5 до 20 тыс. транзакций в секунду [22]. В сравнении, BFT-SMaRt может достичь скорости максимум 10 тыс. транзакций в секунду. В то же время, данная система куда стабильнее выдерживает потенциально вредоносные действия нод блокчейна. В BFT-SMaRt некорректные транзакции не включаются в блоки, так как валидация транзакции происходит перед созданием блока и распространения к пирам. Можно точно сказать, что BFT-SMaRt лучше Raft как по показателям информационной безопасности, так и по показателям производительности, однако, библиотека Java, на которой написан протокол, не предоставляет стабильного сервиса обработки транзакции, и именно из-за этого данная система на текущий момент не включена в Hyperledger напрямую.

Стоит отметить, что протокол консенсуса – это самый критический компонент распределенного реестра. CFT-протоколы считаются не самыми сильными с точки зрения безопасности системы, так как любое злонамеренное действие может повлиять на безопасность сети. BFT-протоколы внедряются в случаях, когда очевидна необходимость в максимально защищенной системе. Тот факт, что каждый пир в блокчейне отвечает за свое поведение, придает нодам стимул соблюдать корректность протокола. Касаемо вопроса распространенных атак на блокчейн Fabric, можно сказать, что в данную систему уже встроена защита от самых популярных консенсусоориентированных атак, таких как атака двойной тратой. Следовательно, для сети, не требующей обеспечения высокого уровня конфиденциальности, можно предложить консолидацию системы Fabric и протокола консенсуса CFT.

Наглядно сравнение данных протоколов представлено в таблице.

4. Безопасность сети

В сетях, где имеется возможность управлять административными доступами, минимизируется возможность нанесения злонамеренного вреда системе со стороны пользователей. В частности, риск компрометации системы вследствие таких атак, как «атака 51 %», «атака Сибиллы», «задержка блока» и «стратегия самозванца», существенно уменьшается [22, 23].

Угрозы сети и спецификация Fabric

Как уже отмечалось ранее, рост популярности Fabric привносит новые риски безопасности, которые могут повредить ее работоспособности и производительности [24]. В данном разделе будут рассмотрены наиболее популярные атаки, которые нацелены на сеть в случае порчи некоторых нод системы, а также указаны контрмеры для увеличения за-

Таблица. ***Сравнение протоколов консенсуса Hyperledger Fabric***

Показатели / Протокол	Производительность	Преимущества	Проблемы протокола
SOLO	Средняя (в зависимости от производительности ноды)	Удобный инструмент для разработки и отладки блокчейн-системы	Единая точка отказа: при отказе одной ноды перестает работать вся система, из-за этого систему необходимо использовать только в целях разработки
KAFKA	Высокая (около 7000–10 000 транзакций в секунду)	Низкая задержка вывода транзакции, хорошие показатели производительности	Достаточно сложная архитектура и неполная децентрализованность системы, возможные проблемы с информационной безопасностью
RAFT	Очень высокая (около 20 000 транзакций в секунду)	Низкая задержка вывода транзакции, на данный момент – лучшие показатели производительности [7]	Возможные проблемы с информационной безопасностью системы
BFT-SMaRt	Высокая (около 10 000 транзакций в секунду)	Хорошие показатели производительности и информационной безопасности	Библиотеки Java, на которых написана система, не предоставляют стабильного сервиса обработки транзакций

щищенности последней. Графически эта информация представлена на рисунке.

1. ***Скомпрометированный поставщик услуг членства (Membership Service Provider, MSP).*** Самый главный и революционный аспект блокчейна – децентрализованность, но Fabric не использует его ввиду своей основной концепции. Централизация HF базируется на MSP и поставщике сертификатов (CA). MSP – это критический элемент платформы, так как он отвечает за регистрацию, идентификацию и виды доступа у нод в блокчейне, таких как клиенты, пиры и даже административные ноды. Следовательно, при взломе или нарушении работы MSP возможны удаление или добавление пользователей в/из сети, а также изменение уровней доступа пользователям сети. Со зловредным MSP неавторизированный доступ, который получает атакующий, может привести к сильному урону и потенциально привести к дальнейшим атакам, таким как «атака некорректной идентификации», «двойная трата», атака на административную ноду и т. д. [24].

2. ***Идентифицированные пиры, подтверждающие транзакции.*** В блокчейне Fabric транзакцию в фазе выполнения должны подтвердить специальные подтверждающие пиры. Взамен данному действию подтверждающие пиры должны идентифицировать себя при помощи подписи, чтобы они смогли подтверждать транзакции и в дальнейших фазах. Однако процесс идентификации пиров в системе HF не лишен и минусов [25, 26], таких как:

- *создание конфликтов:* для некоторых транзакций, подтверждающие пиры могут иметь различные мнения насчет корректности транзакций, а идентифицируя себя, пиры могут инициировать некоторые конфликты внутри своей группы [26];
- *решение большинства:* концепция подтверждения не только не позволяет пирам подтверждать транзакцию в секрете, но и выбирает решение об одобрении большинства;
- *DoS-атаки:* возможны атаки на некоторые подтверждающие пиры, что потенциально может либо замедлить вхождение транзакций в блокчейн, либо ухудшить про-

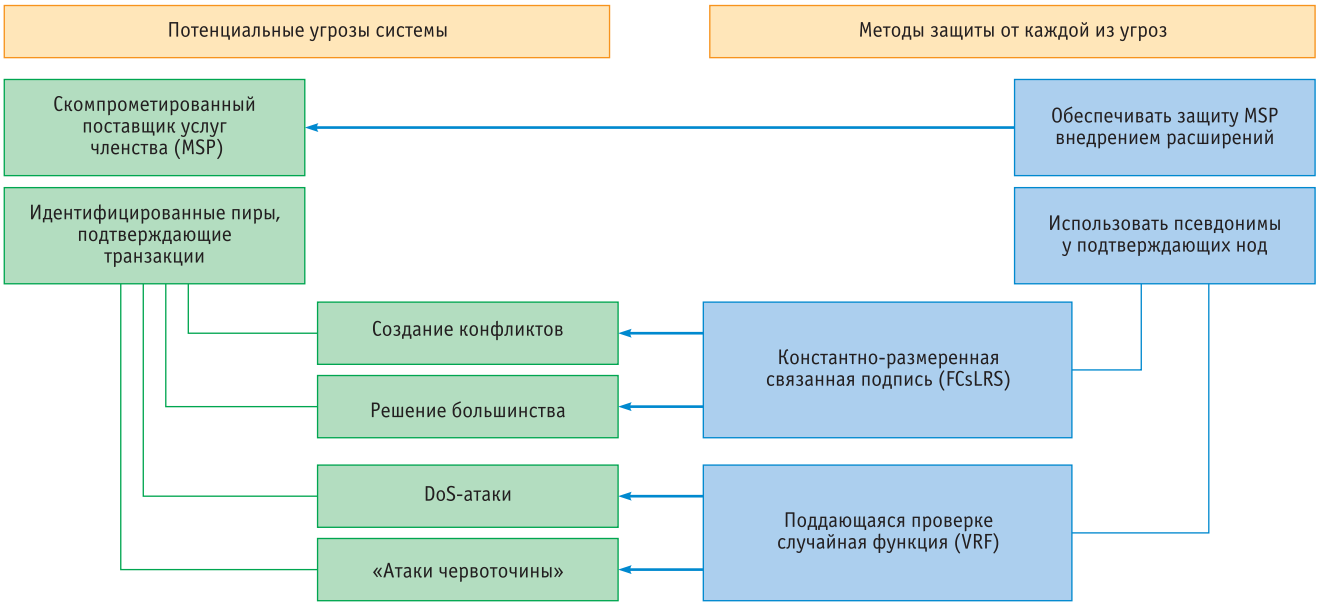


Рисунок. ***Потенциальные угрозы системы HF и методы защиты для каждой из угроз***

изводительность блокчейна в целом [25];

- *«атаки червоточины»:* эта атака, которая может привести к утечке конфиденциальной информации всех пиров в конкретном канале, возможна при злонамеренном действии пира, вступающим в сговор с сообщником вне канала (из этой проблемы можно сделать вывод, что механизм доступа Fabric подразумевает доверие между пирами внутри сети).

Проблемы и открытые вопросы сети блокчейна

Представленный анализ MSP и подтверждающих пиров показывает, что в сети Fabric недостаточно проработаны механизмы уменьшения сетевых рисков. Стоит отметить, что в целом разработка предоставляет собой сильную систему сетевого учета и в совокупности соответствует нормам информационной безопасности. Вместе с тем, исследования в данной области, направленные на ее улучшение, еще продолжаются. Рассмотрим некоторые подходы, которые могут быть использованы в ближайшем будущем для выполнения этой цели.

1. ***Обеспечивать защиту MSP.*** Возможные угрозы, которые могут появиться при скомпрометированном MSP, были проанализированы [26] с использованием технологии расширений защищенности Intel (*Software Guard Extensions*, SGX)[2]. В систему SGX входит техника удаленной идентификации, а также возможность регистрации каждого пользователя системы на доверенных нодах. SGX предоставляет возможность защищать MSP во всех фазах исполнения, таких как регистрация ноды, подписывание транзакции и ее подтверждение. MSP с включенной защитой SGX может также снизить некоторые риски нарушения конфиденциальности и улучшить защиту системы от некоторых возможных атак. Следовательно, необходимо полноценно проанализировать все возможные атаки на сервис членства (MSP и соответствующие компоненты) в целях конкретизации, учета и структурирования.

2. ***Использовать псевдонимы у подтверждающих нод.*** После анализа описанной выше проблемы, касающейся идентификации «подтверждающих пиров», в научной литературе было предложено [25] создать новую «кольцевую» систему подписей под длинным названием «константно-размерная связанная кольцевая подпись Fabric» (*Fabric's Constant-Sized Linkable Ring Signature*, FCsLRS), которая служит для создания псевдоанонимности подтверждающим пирам. Была предложена система подписей на языке программирования GO, а также проведен экспериментальный анализ безопасности и производительности системы. Концепция предложенной подписи состоит в том, что «подтверждающие пиры» подтверждают транзакцию без открытия своей личности, подсчитывая только индивидуальные корректные кольцевые подписи. Другая похожая работа [28] анализирует исход DoS-атаки на «подтверждающие пиры» и предлагает две техники анонимизации: первая использует верифицированную случайную функцию (*Verifiable Random Function*, VRF), а вторая использует псевдонимы. В обоих случаях происходит ухудшение эффективности работы системы с одновременным улучшением уровня ее информационной безопасности за счет анонимизации отправителя и получателя приватной транзакции [25] и обретением системой Fabric полноценной защиты от DoS-атак и «атак червоточины».

5. Сохранение приватности

В текущей концепции технологии блокчейн информация о транзакциях является достоверной (из-за консенсуса) и передаваемой (из-за распределенного реестра). Однако данные преимущества также привносят опасности раскрытия конфиденциальной информации пользователей и организаций. Очевидно, что никакой пользователь не захочет раскрытия свой конфиденциальной информации неавторизованным пользователям в системе, так же как и организации не обрадуются широкой огласке сведений, например, производственных технологиях, зарплатах сотрудников, бухгалтерской отчетности и т. д.

Следовательно, сбор важной информации и ее защищенное хранение в распределенном реестре – это наиважнейшая задача, так как она должна совмещаться с главными регламентами по информационной безопасности. Далее в текущей главе будут рассмотрены механизмы защиты данных в HF, а также предложен ряд важных улучшений, которые необходимо предпринять для дальнейшего совершенствования клиентской конфиденциальности в Hyperledger Fabric.

Fabric поддерживает множество механизмов защиты конфиденциальности системы. Исходя из используемой в ней системы доступа, которая авторизует участвующие в блокчейне сущности сети для аутентификации их личности, могут быть предложены некоторые улучшения для достижения оптимальной конфиденциальности.

1. ***Каналы.*** Канал – это частичный раздел системы со своими правами доступа и механизмом установки порядка транзакций. Каждым каналом управляют несколько пиров, доступы которых совмещаются для работы с соответствующими ресурсами блокчейна (такими как состояние реестра, просмотр включенных транзакций, а также просмотр чейнкода). Когда пир регистрируется в канале, которому соответствует уни-

[2] *Intel Software Guard Extensions (Intel SGX) – набор инструкций центрального процессора, предоставляющих возможность приложению создавать анклавы – области в виртуальном адресном пространстве, защищенные от чтения и записи извне этой области другими процессами, включая ядро операционной системы. Intel SGX обеспечивают целостность и конфиденциальность вычислений с повышенными требованиями к безопасности, производимыми на системах, где привилегированные процессы (ядро операционной системы, гипервизор, и т. д.) считаются ненадежными. Применяется в безопасных удаленных вычислениях, для обеспечения конфиденциальности проприетарных алгоритмов и ключей шифрования, для безопасного просмотра web-страниц и защиты авторских прав.*

кальный идентификатор, на этом же пире создается и запускается соответствующий реестр, позволяющий ему работать с идентичными и постоянно обновляющимися данными, соответствующими данным других пиров. Такие механизмы сохранения конфиденциальности, как каналы, очень важны для предоставления блокчейну решений по консорциуму в сети (когда консорциум поддерживается несколькими организациями или сторонами с общими целями).

2. ***Сбор конфиденциальной информации.*** Пока каналы «работают» над сохранением конфиденциальности информации, позволяя ей храниться разделенным образом, приватный сбор данных (*Private Data Collection,* PDC) способствует обеспечению конфиденциальности информации с другого «ракурса» [3]. PDC создается для того, чтобы предоставлять пирам возможность подтверждать, коммитить и разделять конфиденциальные данные без необходимости создавать новый канал или дополнительную надстройку системы.

PDC – это смесь следующих элементов:

- самих конфиденциальных данных, которые отправляются к (от) авторизованным(ых) пирам(ов) по «протоколу сплетника», содержащимся на приватных базах данных пиров и просматриваемых только этим набором нод, а не административной нодой;
- хэша конфиденциальных данных, который выполняется, заказывается и содержится в каждом из реестров пиров как доказательство существования транзакции (в некоторых случаях, когда пир желает поделиться конфиденциальной информацией с другими пирами, например, чтобы передать информацию третьей доверенной стороне (*Trusted Third Party*, TTP), TTP может создать хэш данной конфиденциальной информации и последовательно изучать вывод значения хэша и сверять его с хэшем, который хранится в реестре канала, тем самым доказывая существование транзакции).

Концепцию «Право быть забытым» можно использовать в конфиденциальных транзакциях, потому что каждый пир способен в любой момент удалить свою собственную локальную базу данных, тем самым уничтожив все данные, но оставив хэши, указывающие на удаленную информацию. Другой аспект введения приватных транзакций – это ограничение их использования. Концепция «Блок для жизни» может быть реализована для каждого приватного сбора данных с целью определения количества времени, которое необходимо затратить на автоматическую очистку каждой скрытой базы данных.

Несмотря на хорошие показатели конфиденциальности, которые демонстрирует PDC, использовать данную надстройку следует с осторожностью, так как метаданные конфиденциальной информации могут предоставить доступ к таковой или даже показать ее содержимое. При таком развитии сценария атаки неавторизованный пир, расположенный в одном канале с атакуемым пиром, может прослеживать общий реестр и фиксировать периодичность появления конфиденциальных транзакций.

Подводя итог, можно констатировать, что некоторые пиры должны иметь полноценный доступ к реестру, а некоторые – частичный. В случае, где данные транзакции остаются скрытыми во время стадии заказа пиров, находящихся в том же канале, что и административная нода, решением является внедрение системы PDC.

6. Заключение

В настоящей статье были описаны и проанализированы наиболее актуальные концепции и контрмеры для уменьшения рисков нарушения информационной безопасности в блокчейн-системе Hyperledger Fabric.

Рассматривая проблему с позиции защищенности протоколов консенсуса, можно сказать, что активное исследование консенсусов группы BFT, таких как BFT-SMaRT, продолжается, так как они могут предоставить существенное улучшение показателей пропускной способности транзакций и защиту от зловредных административных нод. Более того, протоколы BFT еще не были использованы в продуктивных (организационных) средах, и нет сомений, что нам еще предстоит стать свидетелями их применения в реальных блокчейнах.

В статье также были проанализированы некоторые атаки на сеть и предложены активные решения для противоборства таковым. Кроме того, было предложено внедрение концепции расширения защищенности Intel SGX (как альтернативы или надстройки над системой) для защиты от внутренних угроз и DoS-атак, исходящих из манипуляций над выполнением чейнкода системы. Отмечено, что техники для защиты от «атак червоточины» должны содержать в себе анонимизацию отправителей и получателей транзакций внутри каналов.

Так как научные исследования в данной сфере проводятся весьма активно (особенно за рубежом), можно утверждать, что не за горами появление и практическое использование новых надстроек и технологий, таких как, например, внедрение протокола ZKP[3] или постквантовых электронных подписей. Вместе с тем, новые надстройки и механизмы в Hyperledger Fabric, улучшая ее производительность, способствуют появлению и новых угроз безопасности системы, которые следует своевременно выявлять и обезвреживать. ■

[3] *Zero-Knowledge Proof (доказательство с нулевым разглашением) – протокол, который позволяет обмениваться данными между двумя сторонами без использования пароля или любой другой информации, связанной с транзакцией. Использование ZKP является гарантией, что в процесс коммуникации не смогут вмешаться третьи лица и каким-либо образом воздействовать на ее безопасность. Несмотря на то, что суть передаваемой информации не раскрывается, одна сторона все равно может убедиться в том, что с другой – именно тот человек, за которого он себя выдает.*

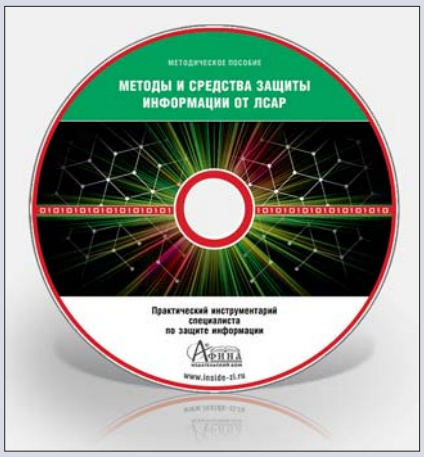
ЛИТЕРАТУРА

1. Nakamoto S., Bitcoin A. A peer-to-peer electronic cash system [Электронный ресурс]. – URL: https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf (дата обращения: 05.07.2022).
2. Brotsis S. et al. Blockchain solutions for forensic evidence preservation in IoT environments // 2019 IEEE Conference on Network Softwarization (NetSoft). – IEEE, 2019. P. 110–114.
3. Ma C. et al. The privacy protection mechanism of Hyperledger Fabric and its application in supply chain finance // Cybersecurity. 2019. V. 2, № 1. P. 1–9.
4. Tian H., He J., Ding Y. Medical data management on blockchain with privacy //Journal of medical systems. 2019. V. 43, № 2. P. 1–6.
5. Kolokotronis N. et al. On blockchain architectures for trust-based collaborative intrusion detection // 2019 IEEE world congress on services (SERVICES). – IEEE, 2019. V. 2642. P. 21–28.
6. Buterin V. et al. A next-generation smart contract and decentralized application platform // White paper [Электронный ресурс]. – URL: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (дата обращения: 05.07.2022).
7. Hyperledger fabric's documentation [Электронный ресурс]. – URL: https://hyperledgerfabric.readthedocs.io/en/release 2.0/orderer/ordering service.html (дата обращения: 05.07.2022).
8. Cachin C. et al. Architecture of the hyperledger blockchain fabric // Workshop on distributed cryptocurrencies and consensus ledgers. – 2016. – Т. 310, № 4. – С. 1–4.
9. Sousa J., Bessani A., Vukolic M. A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform // 2018 48th annual IEEE/IFIP international conference on dependable systems and networks (DSN). – IEEE, 2018. P. 51–58.
10. Чистяков М. А. Hyperledger Fabric: особенности, сферы применения // Аллея науки. – 2018. – Т. 1, № 2. – С. 776–779.
11. Nasir Q. et al. Performance analysis of hyperledger fabric platforms // Security and Communication Networks. 2018. V. 1. P. 1–14.
12. Shalaby S. et al. Performance evaluation of hyperledger fabric // 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). – IEEE, 2020. P. 608–613.
13. Полещук Е. М. и др. Обеспечение приватности и конфиденциальности при разработке смарт-контракта // Молодежь. Наука. Инновации. – 2020. – Т. 1. – С. 200–203.
14. Сосновский Ю. В. Обеспечение целостности ключевых данных в распределенной замкнутой системе управления на основе технологии Blockchain // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации. – 2020. – С. 237–240.
15. Brotsis S. et al. On the security and privacy of hyperledger fabric: Challenges and open issues // 2020 IEEE World Congress on Services (SERVICES). – IEEE, 2020. P. 197–204.
16. Andola N. et al. Vulnerabilities on hyperledger fabric // Pervasive and Mobile Computing. 2019. V. 59. P. 101050.
17. Androulaki E. et al. Hyperledger fabric: a distributed operating system for permissioned blockchains // Proc. of the 13th EuroSys conference. 2018. P. 1–15.
18. Ongaro D., Ousterhout J. In search of an understandable consensus algorithm // 2014 USENIX Annual Technical Conference (Usenix ATC 14). 2014. P. 305–319.
19. Bellini E., Ceravolo P., Damiani E. Blockchain-based e-vote-as-a-service // 2019 IEEE 12th International Conference on Cloud Computing (CLOUD). – IEEE, 2019. P. 484–486.
20. Ferris C. Does Hyperledger Fabric perform at scale? [Электронный ресурс]. – URL: https://www.ibm.com/blogs/blockchain/2019/04/doeshyperledgerfabricperformatscale/ (дата обращения: 05.07.2022).
21. Bessani A., Sousa J., Alchieri E. E. P. State machine replication for the masses with BFT-SMART // 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. – IEEE, 2014. P. 355–362.
22. Gorenflo C. et al. FastFabric: Scaling hyperledger fabric to 20000 transactions per second // International Journal of Network Management. 2020. V. 30, № 5. P. e2099.
23. Yamashita K. et al. Potential risks of hyperledger fabric smart contracts // 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE). – IEEE. 2019. P. 1–10.
24. Davenport A., Shetty S., Liang X. Attack surface analysis of permissioned blockchain platforms for smart cities // 2018 IEEE International Smart Cities Conference (ISC2). – IEEE, 2018. P. 1–6.
25. Andola N. et al. Vulnerabilities on hyperledger fabric // Pervasive and Mobile Computing. 2019. V. 59. P. 101050.
26. Mazumdar S., Ruj S. Design of anonymous endorsement system in hyperledger fabric // IEEE Transactions on Emerging Topics in Computing. 2019. V. 9, № 4. P. 1780–1791.
27. Liang X. et al. Towards a trusted and privacy preserving membership service in distributed ledger using Intel software guard extensions // International Conference on Information and Communications Security. – Springer, Cham. 2017. P. 304–310.

НОВОСТИ

Методы и средства защиты информации от лазерных систем акустической разведки (ЛСАР).

Информационное пособие



Представляемое пособие предназначено для специалистов (инженерно-технических работников) в области технической защиты конфиденциальной информации (ТЗКИ), руководителей работами по защите информации. Также оно рассчитано на широкий круг читателей, в том числе студентов, интересующихся вопросами ТЗКИ.

В пособии рассмотрены:

- классификация методов и средств защиты информации от лазерных систем акустической разведки (ЛСАР);
- имеющиеся нормативные правовые акты, регламентирующие применение ЛСАР и средств защиты от них;
- применение организационных мер обеспечения безопасности;
- технические методы защиты речевой информации от утечки по техническому каналу, связанному с применением лазерных микрофонов;
- современные средства ТЗКИ и особенности их применения на объектах.

Автор – заместитель генерального директора АО «Лаборатория ППШ» А. В. Лысов, к. т. н., доцент – без малого сорок лет занимается данной проблематикой, имеет более 170 публикаций в рассматриваемой области.

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

Метод восстановления облачных и пограничных вычислений на основе кибериммунитета

En **Cloud and Edge Recovery Method Computing Based on Cyber Immunity**

A. A. Balyabin
treven.wt@yandex.ru

S. A. Petrenko,
PhD (Eng., Grand Doctor), Full Professor
s.petrenko@rambler.ru

Saint-Petersburg State Electrotechnical University «LETI»

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

A new method for restoring cloud and edge computing based on cyber immunity is considered, which makes it possible to detect anomalies in computer computing in the event of security threats, counteract cyber attacks (including previously unknown ones) by intruders, perform self-healing of calculations, and also accumulate knowledge for perfection of a «cyber-immune response» to cyber-attacks by intruders in the future. The scientific and practical novelty of the proposed method lies in the ability to accumulate «immune memory», plan the «immune response» procedure and carry out self-healing of cloud and edge computing in quasi-real time, preventing the transition of the cloud critical information infrastructure of the Russian Federation into catastrophic states.

Keywords: cloud critical information infrastructure, information security, threat model, intruder model, MITRE ATT&CK threat matrix, immune response method, cloud computing self-healing methods and algorithms

Рассмотрен новый метод восстановления облачных и пограничных вычислений на основе кибериммунитета, который позволяет выявлять аномалии компьютерных вычислений в случае реализации угроз безопасности, противодействовать кибератакам (в том числе и ранее неизвестным) злоумышленников, осуществлять самовосстановление вычислений, а также накапливать знания для совершенствования «кибериммунного ответа» на кибератаки злоумышленников в будущем. Научная и практическая новизна предлагаемого метода заключается в способности накапливать «иммунную память», планировать процедуру «иммунного ответа» и осуществлять самовосстановление облачных и пограничных вычислений в квазиреальном масштабе времени, препятствуя переводу критической облачной информационной инфраструктуры Российской Федерации в катастрофические состояния.

Ключевые слова: облачная критическая информационная инфраструктура (КИИ), информационная безопасность, модель угроз, модель нарушителя, матрица угроз MITRE ATT&CK, метод иммунного ответа, методы и алгоритмы самовосстановления облачных вычислений

Артем Алексеевич Балябин
treven.wt@yandex.ru

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

Введение

В условиях беспрецедентного роста угроз безопасности и кибератак злоумышленников становится очевидной недостаточная эффективность существующих классических алгоритмов, методов и средств защиты информации. Так, облачная критическая информационная инфраструктура (КИИ) Российской Федерации имеет сложную многоуровневую организацию, что снижает ее прозрачность и усложняет интеллектуальное управление ею. Применяемые на сегодняшний день подходы к обеспечению надежности и отказоустойчивости в большинстве случаев сводятся к внедрению структурно-функциональной избыточности. Такие методы повышения отказоустойчивости, как реконфигурация, *n*-кратное резервирование, эталонирование, репликация, на сегодняшний день не способны в полной мере предотвратить катастрофические последствия для облачной критической информационной инфраструктуры государства и бизнеса в случае реализации угроз безопасности, а методы, сводящиеся к восстановлению из контрольных точек и рестарту вычислительных процессов, могут приводить к длительному

простою или недоступности системы, а также к частичной или полной потере обрабатываемой информации, что недопустимо для систем с высокими требованиями к надежности и отказоустойчивости.

Кроме этого, ландшафт угроз постоянно меняется: выявляются новые уязвимости программного и аппаратного обеспечения облачной инфраструктуры, применяются более сложные техники и тактики нападения, совершенствуются способы обхода средств защиты. Около 40 % от общего количества кибератак относятся к числу ранее неизвестных, не обнаруживаемых существующими системами обнаружения вторжений, системами противодействия компьютерным атакам и иными средствами защиты [1]. Актуальность данной работы обуславливается необходимостью обеспечения киберустойчивости облачных и пограничных машинных вычислений в условиях роста угроз безопасности, а также наделения их способностью противодействовать как известным, так и ранее неизвестным кибератакам.

Степень разработанности темы

Проблема восстановления корректности функционирования информационных систем в условиях вредоносных воздействий и связанные с ней сопроблемы являются предметом изучения отечественных и зарубежных исследователей.

В работах [1–8] рассматриваются возможные решения научно-технической проблемы придания информационным системам свойств, позволяющих предотвратить катастрофические последствия от реализации кибератак злоумышленников. Большое внимание уделено развитию идей кибериммунитета, в частности, изучению и формализации закономерностей его формирования, накопления и применения.

Работы [9, 10] посвящены анализу биологических метафор и подходов, применимых для защиты компьютерных систем, таких как нейронные сети, эволюционные методы, иммунные системы и др., а также предлагаются варианты их комплексирования. В частности, в работе [10] представлена гибридная система обнаружения вторжений, основанная на нейронных сетях, иммунных детекторах и нейронечетких классификаторах. Общим для систем подобного типа является использование для обнаружения злоумышленных воздействий в основном сигнатурных и корреляционных методов, которые обладают высокой точностью при выявлении уже известных или слабо отклоняющихся от известных воздействий. Однако для выявления и своевременного реагирования на ранее неизвестные кибератаки требуется применение иных методов – инвариантных.

Задача выделения признаков поведения программ защищаемой информационной системы (корректное или некорректное поведение), инвариантных относительно условий их функционирования, эквивалентна задаче определения изоморфности двух систем относительно некоторого отображения. Математический аппарат теории подобия и размерностей может применяться для установления необходимых и достаточных условий изоморфности таких систем, а также для определения качественных и количественных параметров изоморфизма.

Основные положения теории подобия формулировались в работах А. А. Гухмана, М. В. Кирпичева, В. А. Веникова, Л. И. Седова применительно к процессам, происходящим в электрических и механических системах [11]. Позднее теория подобия и размерностей была применена и для моделирования вычислительных процессов, в частности, в области кибербезопасности.

Так, в работах [12–16] рассматриваются вопросы, связанные со статической и динамической верификацией вычислительных программ на основе соотношений подобия, в том числе предлагается формировать цифровой паспорт, включающий в себя инварианты подобия, характеризующие расчетные алгоритмы программы, и производить динамический контроль корректности вычислений путем построения аналогичных инвариантов в условиях воздействий и сравнения их с эталонными. Предложенные способы позволяют выявлять нарушения целостности вычислений, вызванные в том числе и ранее неизвестными воздействиями, однако вопросы, связанные с автоматизацией построения цифрового паспорта и накоплением информации о выявленных нарушениях целостности вычислений, в этих работах не рассматривались.

Работа [12] посвящена разработке методов и средств обеспечения устойчивости функционирования программ в условиях вредоносных воздействий. Авторы предлагают метод контроля корректности вычислительных процессов на основе временных автоматов, использующих эталонные профили, являющиеся инвариантами относительно обрабатываемых данных и маршрутов выполнения программ. Стоит отметить, что такой метод позволяет контролировать лишь корректность переходов между линейными участками программы и время их выполнения, что не гарантирует корректности вычислений внутри этих линейных участков.

Работы [8–10] посвящены развитию идей, изложенных в [1–4]. В [11] предложен алгоритм паспортизации программ, а в работах [1–4, 13–16] – алгоритмы обнаружения аномалий на основе теории подобия и размерностей, позволяющие осуществлять контроль семантической корректности вычислений и гарантировать корректность их результатов.

Очевидно, что появление новых уязвимостей и способов их эксплуатации неизбежно по причине постоянного роста сложности программного и аппаратного обеспечения информационных систем. С другой стороны, очевидна необходимость обеспечения требуемого уровня их устойчивости и надежности. С учетом данного противоречия актуальной является задача исследования возможности применения биоинспирированных подходов, в частности, наделения информационных систем свойствами «иммунитета» по аналогии с иммунитетом живого организма для эффективного противодействия как известным, так и ранее неизвестным кибератакам злоумышленников, и упреждения их послед-

ствий. Принципиальным отличием такого подхода от уже существующих является наличие способности накапливать «иммунную память» к уже встречавшимся и вновь появляющимся кибератакам, планировать процедуру «иммунного ответа» и осуществлять самовосстановление в режиме реального времени.

Для разрешения обозначенного противоречия в настоящей статье предложен новый метод восстановления облачных и пограничных вычислений, сущность которого заключается во внедрении в код приложений элементов структурно-функциональной избыточности с последующим их контролем и восстановлением в случае обнаружения аномалий.

Модель облачных и пограничных вычислений в условиях роста угроз безопасности

Рассмотрим два вычислительных процесса p_1 и p_2, представимых уравнениями, имеющими вид:

$$\sum_{i=1}^{q} \varphi_{ui} = 0,\ u = 1, 2, \ldots, r;$$

$$\sum_{i=1}^{q} \phi_{ui} = 0,\ u = 1, 2, \ldots, r,$$

где $\varphi_u = \prod_{j=1}^{n} x\alpha_j^{ui}$ и $\phi_u = \prod_{j=1}^{n} X\alpha_j^{ui}$ и – однородные функции, зависящие от входных параметров вычислительных процессов.

В соответствии с прямой теоремой подобия, если процессы однородно подобны, то справедлива система

$$\frac{\varphi_{ui}}{\varphi_{uq}} = \frac{\phi_{ui}}{\phi_{uq}},$$
$$u = 1, 2, \ldots, r,\ s = 1, 2, \ldots, (q-1).$$

Здесь выражения вида

$$\pi_{us} = \frac{\varphi_{ui}}{\varphi_{uq}}$$

описывают так называемые критерии подобия (инварианты), которые, в соответствии с теоремой подобия, численно равны для взаимно подобных вычислительных процессов. Таким образом, равенство критериев подобия является необходимым условием отнесения вычислительных процессов к подклассу взаимно подобных. Обратная теорема подобия формулирует достаточные условия и гласит, что два процесса однородно подобны, если их полные уравнения возможно привести к виду, в котором инварианты подобия численно равны.

Представим вычислительный процесс P в виде:

$$P = <T, X, Y, Z, F, \Phi>,$$

где T – моменты времени t, в которые осуществляется наблюдение за вычислительным процессом;

X – множество входных параметров вычислительного процесса;

Y – множество выходных параметров вычислительного процесса;

Z – множество $Z_{kj}(j = \overline{1, m})$ состояний вычислительного процесса, характеризующихся в каждый момент времени $t \in T$ выполняемыми в определенной последовательности в контрольной точке k арифметическими операциями;

F – множество операторов перехода f_i, отвечающих за изменение состояния вычислительного процесса;

Φ – множество операторов выхода ϕ_i, отвечающих за формирование результатов вычислений.

Для определения отношений между описанными множествами введем отображения:

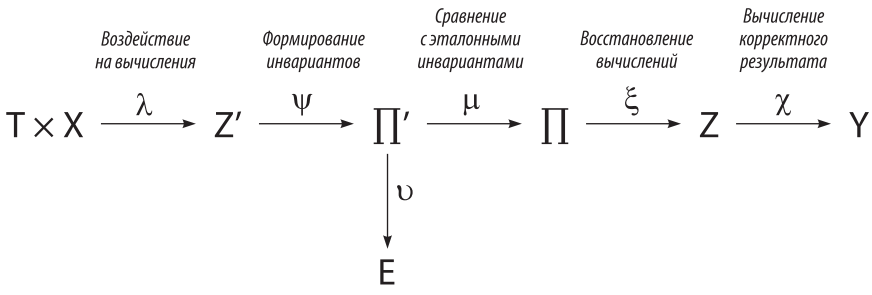


Рис. 1. ***Общий вид диаграммы отображений облачных и пограничных вычислений с восстановлением***

$\lambda : T \times X \to Z'$ – отображение, действующее из множества входных параметров вычислительного процесса X, определяемых в моменты времени T, в множество состояний вычислительного процесса Z' и определяющее воздействия на вычислительный процесс;

$\psi : Z' \to \prod'$ – отображение, действующее из множества состояний вычислительного процесса Z' в множество инвариантов подобия $\prod'$ и определяющее формирование инвариантов подобия в условиях воздействий;

$\mu : \prod' \to \prod$ – отображение, действующее из множества инвариантов подобия в условиях воздействий $\prod'$ в множество эталонных инвариантов $\prod$ и определяющее сравнение их между собой;

$\upsilon : \prod \to E$ – отображение, действующее из множества инвариантов подобия $\prod$ в множество ошибок E и определяющее сигнал о нарушении целостности вычислений;

$\zeta : \prod \to Z$ – отображение, действующее из множества инвариантов подобия $\prod$ в множество состояний вычислительного процесса Z и определяющее восстановление вычислений;

$\zeta : Z \to Y$ – отображение, действующее из множества состояний Z в множество выходных параметров вычислительного процесса Y и определяющее вычисление корректного результата.

Тогда процесс облачных и пограничных вычислений с учетом внешних воздействий, обнаружения аномалий и восстановления можно представить, как показано на рис. 1.

Для контроля семантической корректности облачных и пограничных вычислений необходимо построить граф потока управления (ГПУ) соответствующих приложений:

$$\Gamma(B, D),$$

где $B = \{B_i\}$ – множество линейных участков программы (вершины ГПУ);

$D = \{B \times B\}$ – множество связей по управлению между линейными участками (дуги ГПУ).

Каждый линейный участок $B_i \times B$ ГПУ характеризуется определенной последовательностью арифметических операторов:

$B_i = (b_{i_1}, b_{i_2}, \ldots, b_{il})$.

Каждому элементарному пути в ГПУ соответствует упорядоченная последовательность выполняемых линейных участков:

$B^k = (B_1^k, B_2^k, \ldots, B_t^k)$,

где $B_k \in B$ и $B_i^k = (b_{i_1}^k, b_{i_2}^k, \ldots, b_l^k)$, $\forall i = \overline{1, p}$ есть последовательность арифметических операторов, выполняемых на линейном участке программы – реализация или вычислительный процесс, – которая является фрагментом программы, потенциально подверженным вредоносным воздействиям в виде искажения арифметических операторов.

Представление алгоритма облачных и пограничных вычислений в виде ГПУ необходимо для того, чтобы все арифметические операторы оказались внутри линейных участков и не были связаны с операторами переходов между ними. Это позволяет внедрить контрольные точки с целью расчета соотношений подобия для каждого линейного участка и определения пути в ГПУ. Таким образом, достигается не только контроль целостности потока управления, но и контроль целостности облачных и пограничных вычислений на линейных участках.

Применение теории подобия и размерностей для контроля корректности облачных и пограничных вычислений

Исследования, проведенные в работах [1–4], показали, что проверка соотношений, опирающихся на свойства вычислений, является наиболее эффективным способом контроля корректности облачных и пограничных вычислений, поскольку они задают семантические связи между объектами приложений, вычислимы в динамике их выполнения, и, кроме того, инвариантны относительно входных данных и путей выполнения приложений. Однако задача вычисления инвариантов подобия на основе различных представлений программ является слабо поддающейся формализации.

Обозначим за $f_i^k(x_1, x_2, \ldots, x_N)$ первичное соотношение, соответствующее группе арифметических операторов. Тогда для k-й реализации УГП B^k возможно записать последовательность первичных соотношений в виде:

$$\begin{cases} y_1 = f_i^k(x_1, x_2, \ldots, x_N), \\ y_2 = f_i^k(x_1, x_2, \ldots, x_N, y_1), \\ \ldots \\ y_M = f_M^k(x_1, x_2, \ldots, x_N, y_1, y_2, \ldots, y_{M-1}). \end{cases}$$

Выполним суперпозицию $\{y_i\}$ в правых частях выражений и получим систему соотношений, инвариантных относительно перестановок:

$$\begin{cases} y_1 = z_1^k(x_1, x_2, \ldots, x_N), \\ y_2 = z_2^k(x_1, x_2, \ldots, x_N), \\ \ldots \\ y_m = z_m^k(x_1, x_2, \ldots, x_N). \end{cases} \quad (1)$$

Каждое i-е соотношение

$y_i = z_i^k(x_1, x_2, \ldots, x_N)$

можно представить в виде суммы степенных одночленов:

$$y_i = \sum_{i=1}^{p} z_{ij}(x_1, x_2, \ldots, x_N),$$

где $z_{ij}(x_1, x_2, \ldots, x_N)$ – степенной одночлен.

Слагаемые суммы (1) должны иметь одинаковые размерности, то есть должно выполняться равенство:

$[y_i] = [z_{ij}(x_1, x_2, \ldots, x_N)]$, $i = \overline{1, p_i}$

или

$[z_{ij}(x_1, x_2, \ldots, x_N)] = [z_{il}(x_1, x_2, \ldots, x_N)]$, $i = \overline{1, p_i}$. (2)

Система (2) называется системой определяющих соотношений.

Зададим функцию $\rho = X \to [X]$, которая каждому $x_j \in X$ ставит в соответствие его абстрактную размерность $[x_j] \in [X]$. Тогда размерности в выражении (2) выразятся как

$$[z_{ij}(x_1, x_2, \ldots, x_N)] = \prod_{n=1}^{N} [x_n]^{\lambda_{jn}}, \quad i = \overline{1, p_i}.$$

Используя (1) и (2), построим систему соотношений:

$$\prod_{n=1}^{N} [x_n]^{\lambda_{jn}} = \prod_{n=1}^{N} [x_n]^{\lambda_{ln}}, \; j, \; i = \overline{1, p_i},$$

или

$$\prod_{n=1}^{N} [x_n]^{\lambda_{jn} - \lambda_{ln}} = 1, \; j, \; i = \overline{1, p_i}. \quad (3)$$

Логарифмируя выражения системы (3), получим систему линейных однородных уравнений, называемую критерием семантической корректности:

$$\sum_{n=1}^{N} (\lambda_{jn} - \lambda_{ln}) \ln[x_n] = 0, \; j, \; i = \overline{1, p_i}. \quad (4)$$

Выполнив подобное (4) преобразование для $\forall B_i^k \in B^k$, получим систему однородных уравнений k-й реализации вычислительного процесса:

$A^k \omega = 0$.

Для формирования цифрового паспорта облачных и пограничных вычислений необходимо учитывать различные возможные реализации вычислительных процессов. В общем случае программа представляется совокупностью взаимосвязанных функциональных модулей, предназначенных для решения определенной задачи. Каждая отдельная реализация $B_i^k \in B^k$ является частным решением такой задачи, соответствующим последовательности арифметических операций при входных данных X. Поскольку последовательности арифметических операций, соответствующие различным реализациям, могут частично совпадать, то есть $B^k \cap B^l \neq \varnothing$, $\forall B^k, B^l \in B$, то математические зависимости между группами арифметических операторов при переходе между этими реализациями также должны сохраняться, что позволяет говорить об общности критериев подобия. Исходя из этого, q матриц $\{A^k\}$, соответствующих реализациям $\{B^k\}$, возможно объединить в систему:

$$A = \begin{pmatrix} A_1 \\ \ldots \\ A_q \end{pmatrix}.$$

Такая система представляет собой базу данных эталонных инвариантов для линейных участков программы и является частью ее паспорта. При анализе исполняемого файла инварианты внедряются в него в качестве контрольных точек с целью последующего контроля размерностей в процессе выполнения программы. В каждой контрольной точке управление передается библиотеке паспорта для расчета фактических семантических инвариантов и сравнения их с эталонными. Если получен-

ные инварианты совпадают, управление возвращается выполняемой программе. В противном случае формируется сигнал нарушения целостности вычислений, после чего осуществляется выработка плана восстановления и запоминание обнаруженного нарушения. На рис. 2 представлена схема механизма контроля паспортизированного вычислительного процесса.

Методика контроля и восстановления корректности облачных и пограничных вычислений

Общая схема методики приведена на рис. 3.

В исполняемый код программы на этапе трансляции (компиляции) встраиваются контрольные точки, сформированные на основе соотношений, сформулированных в терминах теории размерностей и подобия, предназначенные для контроля корректности облачных и пограничных вычислений на критических участках программы. Информация о контрольных точках, эталонных соотношениях подобия (инвариантах), допустимых маршрутах выполнения составляет цифровой паспорт соответствующих приложений. В процессе функционирования кибериммунной системы защиты и противодействия выявляемым кибератакам злоумышленников в системе появляется информация о типах и характеристиках воздействия. Для ее накопления с целью оперативного распознавания и реагирования на угрозы данного типа в будущем в систему иммунной защиты входит подсистема хранения новых знаний кибериммунитета. При обнаружении нарушения целостности вычислений (отклонения потока управления от допустимых декларированных маршрутов, подмены вычислительных операторов и др.), осуществляется классификация характера нарушения и поиск его источника. В случае, если в базе данных кибериммунитета не содержится информации о вредоносном воздействии, запускается процедура самообучения и формирования новых знаний о выявленных нарушениях. По результатам анализа нарушения осуществляется синтез микропрограмм и запускается процедура восстановления облачных и пограничных вычислений, сводящаяся к точечным воздействиям, направленным на возврат вычислительного процесса в корректное состояние. Точечное воздействие позволяет восстановить искаженные вычисления без необходимости перезапуска вычислительного процесса, что минимизирует риски потери обрабатываемой информации и повышает оперативность восстановления облачных и пограничных вычислений.

Заключение

Рассмотренный новый метод восстановления облачных и пограничных вычислений на основе приобретаемого кибериммунитета позволяет выявлять аномалии поведения облачных систем и платформ обработки данных, возникающие в ходе кибератак злоумышленников (в том числе и ранее неизвестных), за счет реализации механизмов иммунной защиты, противодействовать этим атакам, осуществлять самовосстановление параметров поведения, влияющих на киберустойчивость облачных систем и платформ критической информационной инфраструктуры Российской Федерации, а также накапливать знания о злоумышленных воздействиях на КИИ для повышения эффективности реализации «иммунного ответа» на вторжения в будущем. ■

ЛИТЕРАТУРА

1. *Петренко С. А. Кибериммунология: научная монография. – СПб: Издательский дом «Афина» . – 2021. – 240 с.*
2. *Petrenko S. Cyber Resilience. – Denmark (Gistrup): River Publishers. 2019. – 444 p.*
3. *Петренко С. А., Ступин Д. Д. Национальная система раннего предупреждения о компьютерном нападении: научная монография; [под общей редакцией С. Ф. Боева]. – Иннополис, СПб: Издательский дом «Афина». – 2017. – 440 с.*
4. *Петренко С. А. Обзор методов иммунной защиты Индустрии 4.0 // Защита информации. Инсайд. – 2019. – № 5 (89). – С. 36–48.*
5. *Petrenko S. Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation. – Cham, Switzerland: Springer International Publishing. 2018. – 249 p. DOI: 10.1007/978-3-319-79036-7.*
6. *Petrenko S. Cyber resilient platform for Internet of things (IIOT/IOT)ed systems: survey of architecture patterns // Voprosy Kiberbezopasnosti. 2021.*

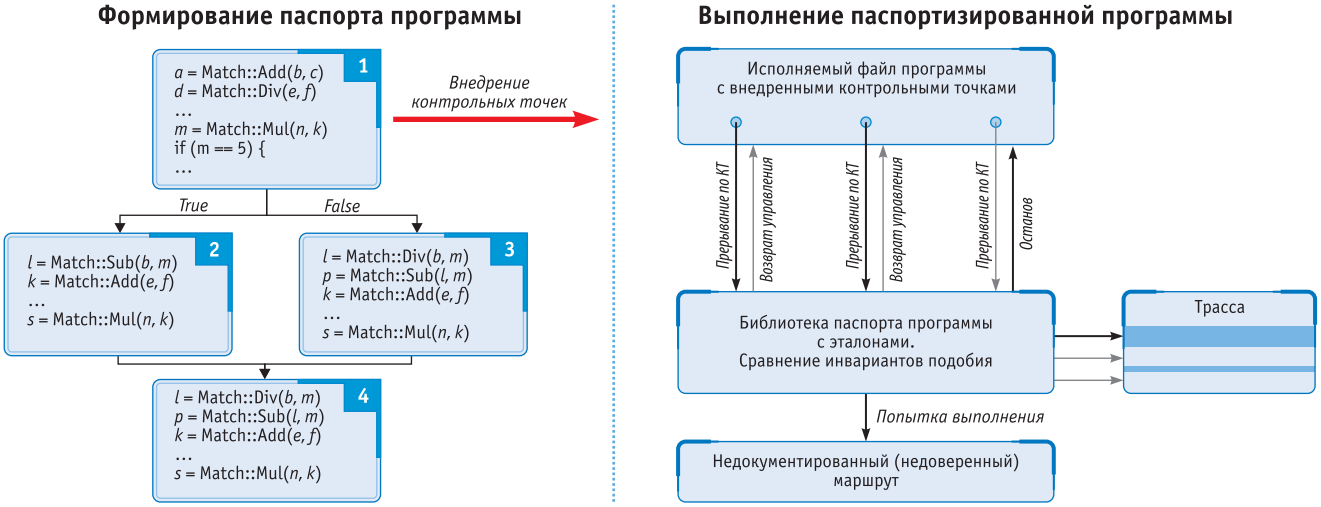


*Рис. 2. **Механизм контроля паспортизированного вычислительного процесса***

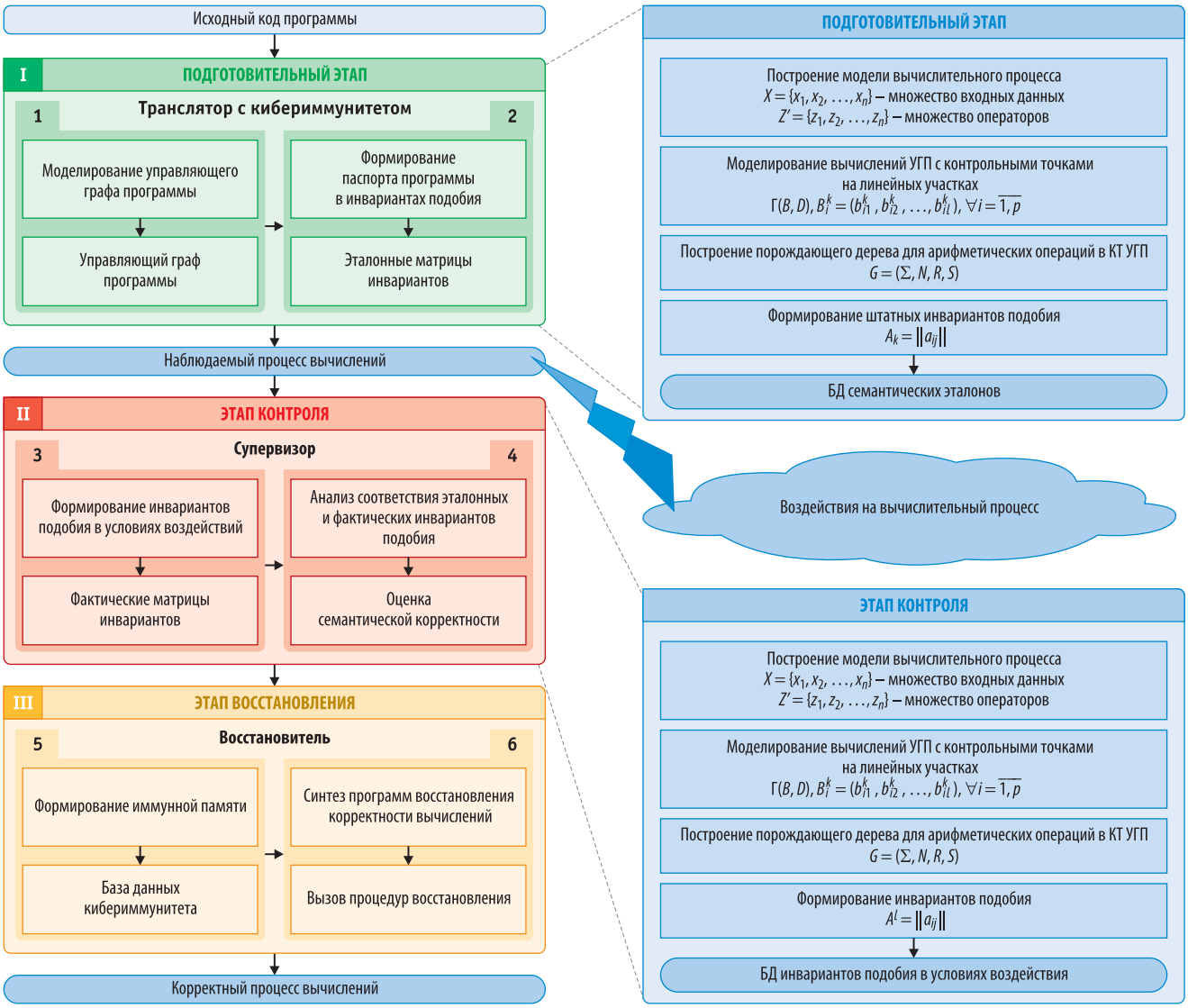


Рис. 3. ***Общая схема методики контроля и восстановления корректности облачных и пограничных вычислений***

№ 2 (42). P. 81–91. DOI: 10.21681/2311-3456-2021-2-81-91.

7. Petrenko A. S., Petrenko S. A., Makoveichuk K. A., Chetyrbok P. V. Protection model of PCS of subway from attacks type «Wanna Cry», «Petya» and «Bad Rabbit» // 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2018. P. 945–949.

8. Petrenko S. A., Stupin D. D. Analytical Verification of Computational Programs // 2018 Engineering and Telecommunication (EnT-MIPT), IEEE, Moscow, Russia. 2018. P. 127–129. DOI: 10.1109/EnT-MIPT.2018.00046.

9. Котенко И. В., Нестерук Ф. Г., Шоров А. В. Методы защиты компьютерных сетей на основе биоинспирированных подходов (Обзор) // Вопросы защиты информации. – 2012. – № 2 (97). – С. 35–46.

10. Браницкий А. А., Котенко И. В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов // Информационно-управляющие системы. – 2015. – № 4 (77). – С. 69–77. DOI: 10.15217/issn1684-8853.2015.4.69.

11. Кирпичев М. В. Теория подобия. – М.: Изд-во Акад. наук СССР. – 1953. – 96 с.

12. Ковалев В. В., Компаниец Р. И., Новиков В. А. Верификация программ на основе соотношений подобия // Труды СПИИРАН. – 2015. – № 1 (38). – С. 233–245.

13. Петренко С. А., Костюков А. Д. Методика гибридного мониторинга угроз безопасности // Защита информации. Инсайд. – 2020. – № 2 (92). – С. 4–16.

14. Балябин А. А., Петренко С. А., Якимовская Р. Н. Алгоритм паспортизации вычислений SAP HANA на основе размерностей // Повышение конкурентоспособности социально-экономических систем в условиях трансграничного сотрудничества регионов: Сб. материалов IX междунар. науч.-практ. конф., Ялта, 05–08 апреля 2022 года; [отв. ред. А. В. Олифиров]. – Симферополь: ООО «Издательство Типография «Ариал». – 2022. – С. 68–71.

15. Балябин А. А., Петренко С. А., Антонов В. В. Алгоритм обнаружения аномалий функционирования SAP HANA на основе размерностей // Повышение конкурентоспособности социально-экономических систем в условиях трансграничного сотрудничества регионов: Сб. материалов IX междунар. науч.-практ. конф., Ялта, 05–08 апреля 2022 года; [отв. ред. А. В. Олифиров]. – Симферополь: ООО «Издательство Типография «Ариал». – 2022. – С. 61–64.

16. Балябин А. А., Петренко С. А., Голумбовская А. Н. Алгоритм выявления аномалий функционирования системных приложений в условиях отсутствия исходных кодов // Повышение конкурентоспособности социально-экономических систем в условиях трансграничного сотрудничества регионов: Сб. материалов IX междунар. науч.-практ. конф., Ялта, 05–08 апреля 2022 года; [отв. ред. А. В. Олифиров]. – Симферополь: ООО «Издательство Типография «Ариал». – 2022. – С. 65–68.

Модифицированная имитационная модель контроля управляющих действий персонала на основе данных сетевого трафика

En **Modified Imitating Model of Control of Personnel Management Actions Based on Network Traffic Data**

T. V. Abramova,
Senior Lecturer
taya357@gmail.com

T. Z. Aralbaev,
Doctor of Technical Sciences, Professor
atz1953@gmail.com

I. D. Zaichikov,
Undergraduate Student
ilya.zaychikov@list.ru

Orenburg State University

The article is devoted to the issues of modeling the process of monitoring the actions of personnel related to the administration of computer networks and information processes in an automated system based on network traffic data.

In the course of the study, a simulation model and an algorithm for personnel control transactions were built, allowing to expand the list of controlled actions, and an experiment was conducted that confirmed the operability of the mathematical model when working with data close to real industrial traffic. Recommendations for detecting unregulated transactions based on network traffic data are proposed.

Keywords: information protection, personnel control actions, automated control systems, network traffic, industrial protocols, associative memory

Статья посвящена вопросам моделирования процесса мониторинга действий персонала, связанных с администрированием компьютерных сетей и информационных процессов в автоматизированной системе по данным сетевого трафика. В ходе исследования построена имитационная модель и алгоритм контроля управляющих транзакций персонала, позволяющие расширить перечень контролируемых управляющих воздействий, а также проведен эксперимент, подтвердивший работоспособность математической модели при работе с данными, приближенными к реальному промышленному трафику. Предложены рекомендации по обнаружению нерегламентированных транзакций по данным сетевого трафика.

Ключевые слова: защита информации, контроль управляющих действий персонала, автоматизированные системы управления, сетевой трафик, промышленные протоколы, ассоциативная память

Таисия Вячеславовна Абрамова,
старший преподаватель
t.v.abramova75@gmail.com

Ташбулат Захарович Аралбаев,
доктор технических наук, профессор
atz1953@gmail.com

Илья Дмитриевич Зайчиков,
магистрант
ilya.zaychikov@list.ru

Оренбургский государственный университет

Основным требованием, определяющим эффективность управляющих систем, является корректное выполнение регламентированных управляющих программ и отдельных команд персоналом. Данное требование в настоящее время приобретает особую актуальность в территориально распределенных автоматизированных системах управления (АСУ) из-за дистанционного характера мониторинга технологических объектов, специфики полевых условий работы персонала и необходимости оперативного принятия решений. По этой причине задачи мониторинга управляющих действий в АСУ с применением эффективных методов и средств регулярно находят отражение в современной научной литературе, в частности, в работах [4, 5, 7].

Одним из недостатков рассматриваемых систем мониторинга является невысокая оперативность средств контроля в условиях реального времени. Вопросы повышения производительности процедур контроля на базе аппаратных средств, по мнению авторов, нуждаются в дальнейших исследованиях и внедрении результатов в распределенных сетевых системах АСУ.

Настоящая работа является продолжением исследований, представленных в публикациях [1, 3]. В ней

изложены результаты разработки модифицированной модели, соответствующего алгоритмического и программного обеспечения, ориентированного на мониторинг действий персонала распределенных АСУ транспортировкой нефтегазового сырья.

Целью работы является снижение рисков от нерегламентированных действий пользователей промышленной сети на основе анализа сетевого трафика. Для достижения цели:

- построена имитационная модель и алгоритм контроля управляющих транзакций персонала, позволяющие расширить перечень контролируемых управляющих воздействий;
- проведен эксперимент и предложены рекомендации по обнаружению нерегламентированных транзакций по данным сетевого трафика.

Под управляющей транзакцией понимается конечная последовательность логически связанных операций оператора или диспетчера, сопряженная, например, с переключением исполнительных механизмов системы и изменением режимов работы трубопровода. Все контролируемые транзакции условно делятся на два класса: регламентированные (*Treg*) и нерегламентированные (*Tunreg*). К последним относятся транзакции, не соответствующие установленным политикам безопасности на объекте.

Особенностью рассматриваемой задачи является необходимость анализа больших объемов сетевого трафика как основного источника информации о состоянии системы [3]. Анализ известных методов мониторинга больших объемов сетевых данных позволил выбрать в качестве базовой модель контроля транзакций на основе ассоциативной памяти (АП), обеспечивающую удобство описания логических условий и повышенную оперативность контроля. Эффективность использования ассоциативной памяти исследована в работах [2, 3].

Математическая модель контроля транзакций персонала включает:

- множество Q контролируемых транзакций:
  $Q = \{q_1, q_2, \ldots, q_j, \ldots q_M\}$,
  где M – число транзакций;
- множество операций в транзакции
  $O = \{o_1, o_2, o_3, \ldots, o_N\}$,
  где N – число операций;
- множество K информативных признаков транзакции:
  $P = \{p_1, p_2, \ldots, p_i, \ldots, p_K\}$.

В качестве основных признаков распознавания транзакции использованы:

- IP – адрес источника транзакции;
- KT – код транзакции;
- NO – номер операции в транзакции;
- KO – код операции.

Кортеж значений перечисленных признаков, полученный по данным сетевого трафика, представленный выражением (1), формирует кодовую сигнатуру S для распознавания легитимности операции в транзакции. Код сигнатуры используется в качестве адреса АП, по которому считывается код соответствующей легитимной операции. В таблице на примере одной транзакции $KT1$, задаваемой с пульта управления с сетевым адресом $IP1$, показана схема формирования адресной части АП. Содержимое ячеек АП формируется администратором АСУ.

В процессе контроля проверяется совпадение кода адресной части KO и кода содержимого ячейки <KO>. Несоответствие кодов KO и <KO> свидетельствует о нелегитимности этой операции, в частности, и всей транзакции в целом.

Особенностью данной системы адресации является включение в адресную часть параметра H, значение которого увеличивается на единицу для каждой последующей операции в случае легитимности предыдущей, что обеспечивает контроль заданной очередности выполнения операций.

Процедура контроля транзакции T описывается выражениями (1) – (5), в которых приняты следующие условные обозначения:

- A_{IP}, A_{KT}, A_{NO}, A_{KO}, A_H представляют собой области допустимых значений, соответственно, для IP, KT, NO, KO и H;
- Y_O, X_{IP}, X_{KT}, X_{NO}, X_{KO}, X_H представляют собой, соответственно, функцию и аргументы легитимности операции (см. врезку).

Операция транзакции из множества O считается легитимной в случае, если значение соответствующей функции Y_o равно единице. Значения аргументов функции Y_o (3) равны единице в случае принадлежности параметров сигнатуры S из выражения (1) соответствующей области допустимых значений из множества A (2). В выражении (4) приведено правило определения легитимности операции по аргументу X_{IP}. Опреде-

Таблица. ***Система адресации в АП в режиме контроля транзакции***

Адрес ячейки АП					Содержимое ячейки
IP	KT	NO	H	KO	<KO>
IP1	KT1	NO1.1	H1.1	KO1.1	KO1.1
IP1	KT1	NO1.2	H1.2	KO1.2	KO1.2
…	…	…	…	…	…
IP1	KT1	NO1n	H1n	KO1n	KO1n

Врезка

$$S = IP\_\ KT\_\ NO\_\ KO\_\ H; \quad (1)$$

$$A = \{A_{IP}, A_{KT}, A_{NO}, A_{KO}, A_H\}; \quad (2)$$

$$Y_o = X_{IP} \wedge X_{KT} \wedge X_{NO} \wedge X_{KO} \wedge X_H; \quad (3)$$

$$X_{IP} = \begin{cases} 1, \text{ если } X_{IP} \in A_{IP} \\ 0, \text{ если } X_{IP} \notin A_{IP}; \end{cases} \quad (4)$$

$$Y_T = \prod_{i=1}^{N} Y_i;\ i = 1, N;\ T \in \begin{cases} T_{reg}, \text{ если } Y_T = 1 \\ T_{unreg}, \text{ если } Y_T = 0. \end{cases} \quad (5)$$

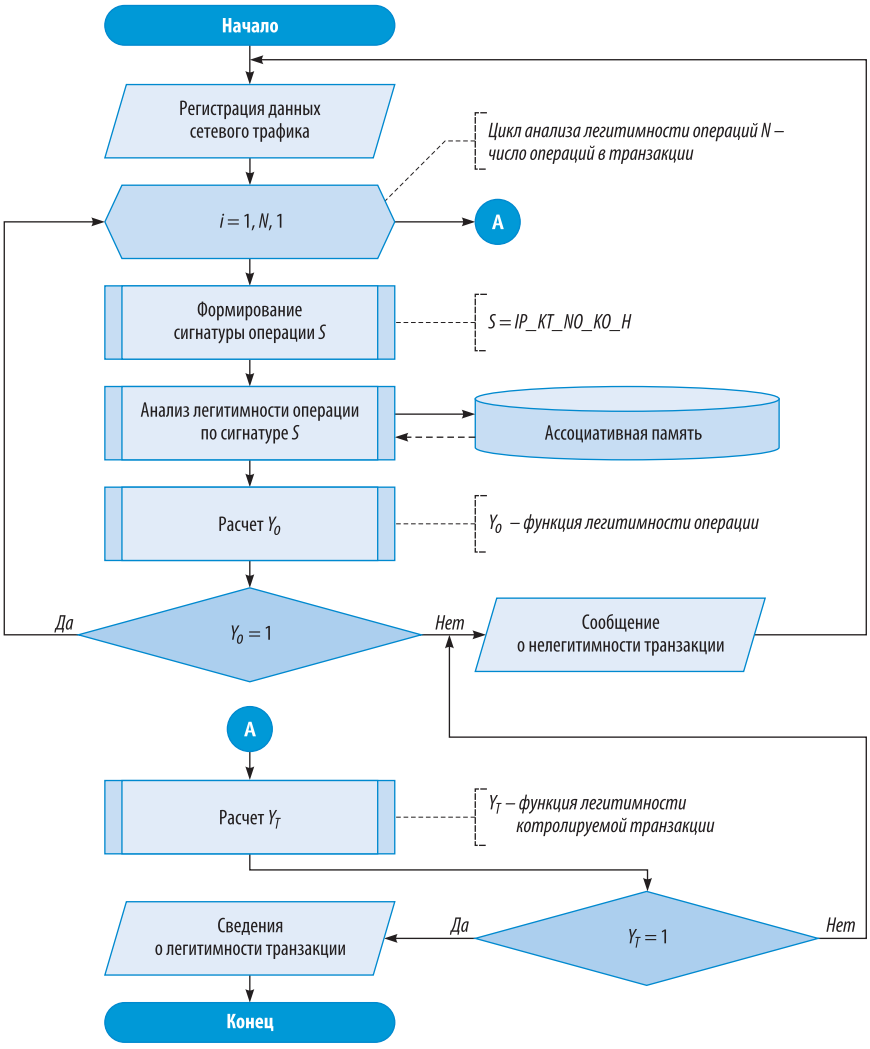


Рис. 1. ***Схема алгоритма контроля управляющей транзакции персонала по данным сетевого трафика***

ление легитимности по аргументам X_{KT}, X_{NO}, X_{KO} и X_H производится аналогично. Транзакция T относится к множеству регламентированных *Treg* в случае истинности функции легитимности транзакции Y_T, согласно выражениям (5).

Схема алгоритма контроля управляющей транзакции персонала на базе разработанной модели представлена на рис. 1.

На первом этапе работы алгоритма производится регистрация пакетов сетевого трафика по протоколу Modbus TCP и формирование сигнатуры S операции, согласно выражению (1). Далее по выражениям (3) – (4) на основе сведений, хранящихся в АП, определяется легитимность операции с использованием соответствующих сигнатур. Цикл анализа транзакции завершается, когда достигнуто конечное число операций N. В случае корректного выполнения всех операций производится расчет функции легитимности транзакции по выражениям (5).

Алгоритм положен в основу программного средства [6] для мониторинга управляющих действий персонала. Экранная форма работы программы представлена на рис. 2. Для апробации программы проведен эксперимент на модельных данных сетевого трафика сегмента информа-

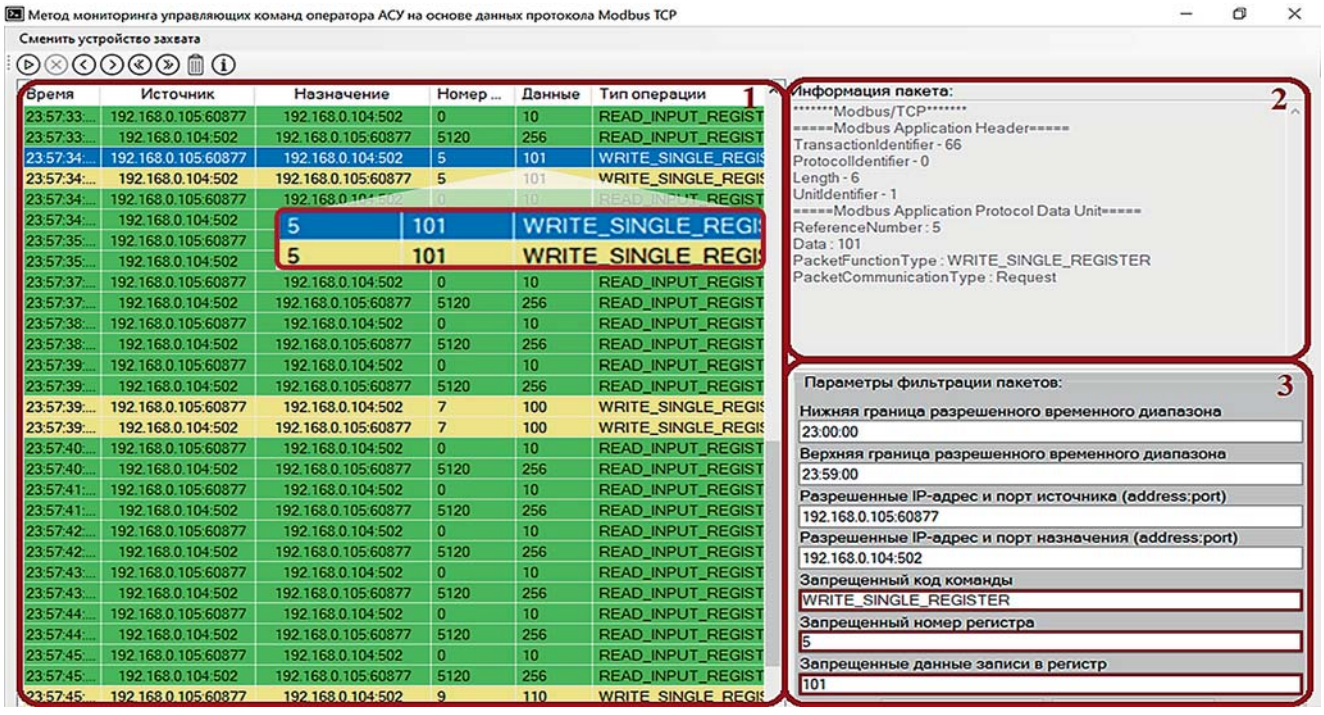


Рис. 2. ***Экранная форма процедуры контроля управляющих транзакций персонала***

ционно-управляющей подсистемы АСУ транспортировкой нефтегазового сырья, построенного с использованием следующих средств:

- программного комплекса Scada Trace Mode, на базе которого разработана мнемосхема участка нефтепровода, имитирующая работу датчиков и исполнительного механизма программ-эмуляторов промышленного протокола Modbus TCP (Modbus Pool и Modbus Slave) для моделирования работы контроллера и автоматизированного рабочего места оператора;
- программы мониторинга управляющих операций оператора АСУ [6].

По завершении эксперимента проведен анализ данных трафика промышленной сети, содержащего сведения о нерегламентированной управляющей транзакции, также представленные на рис. 2.

Анализ результатных данных показал наличие последовательности операций, содержащих нерегламентированные значения, записываемые в регистры контроллера. В частности, зарегистрирована попытка записи данных «101» в регистр «5», запрещенных настройками безопасности в поле 3. В поле 2 выведены сведения о соответствующей операции, формирующие сигнатуру распознавания ее легитимности.

Проведенный эксперимент подтвердил работоспособность математической модели при работе с данными, приближенными к реальному промышленному трафику. Программное средство, разработанное на базе модели, позволило оперативно обнаружить и предупредить неквалифицированные действия персонала.

Достоинством модифицированной модели являются:

- универсальность применения в задачах исследования управляющих действий персонала АСУ, в частности, возможность контроля управляющих операций в различных диапазонах времени, адресов и кодов команд;
- снижение рисков от неквалифицированных действий персонала за счет оперативного контроля управляющих транзакций;
- возможность применения модели в ходе обучения студентов и персонала АСУ задачам безопасности автоматизированного управления.

На основе представленной модели разработаны метод и устройство мониторинга управляющих действий персонала АСУ [8], позволяющие снизить риски от нерегламентированных действий пользователей промышленной сети. ■

ЛИТЕРАТУРА

1. *Абрамова Т. В., Аралбаев Т. З. Модель контроля транзакций пользователя АСУ ТП на основе сигнатурного принципа // Инновационные, информационные и коммуникационные технологии: сб. трудов XVI междунар. науч.-прак. конф.; Сочи. – 2020. – С. 181–185.*
2. *Аралбаев Т.З., Абрамова Т. В. Исследование эффективности методов мониторинга сетевого трафика на основе последовательного и ассоциативно последовательного принципов поиска актуальной информации // СТИН. – 2017. – № 11. – С. 2–5.*
3. *Аралбаев Т. З., Абрамова Т. В. Контроль пользователя в АСУ ТП на основе принципов ассоциативности и мажоритарности // Актуальные задачи фундаментальных и прикладных исследований: материалы Междунар. науч.-практ. конф., 20 нояб. 2018 г. – Оренбург: ОГУ. – 2018. – С. 37–40.*
4. *Горбачев И. Е., Глухов А. П. Моделирование процессов нарушения информационной безопасности критической инфраструктуры // Труды СПИИРАН. – СПб. – 2015. – С. 112–135.*
5. *Каскинов И. И. Ассоциативно-мажоритарная модель системы контроля поведения пользователя на основе теории автоматов // Научное сообщество студентов: Междисциплинарные исследования: сб. ст. по мат. XXII междунар. студ. науч.-практ. конф., № 11 (22) [Электронный ресурс]. – URL: https://sibac.info/archive/meghdis/11(22).pdf (дата обращения: 11.11.2021).*
6. *Абрамова Т. В., Зайчиков И. Д. Метод мониторинга управляющих команд оператора АСУ на основе данных протокола Modbus TCP // Свид-во о гос. регистрации программы для ЭВМ № 2022661790. – 2022.*
7. *Леденев А. В., Колотинский Е. Б., Игнатьев К. С. Система и способ адаптивного управления и контроля действий пользователя на основе поведения пользователя // Патент РФ RU 2534935 C2. – 2014.*
8. *Абрамова Т. В., Аралбаев Т. З., Каскинов И. И., Хатеев М. Д. Устройство для контроля поведения пользователя // Патент РФ RU 2675896 C1. Бюл. № 36. – 2018.*

НОВОСТИ

Кибернетические и информационные войны: основные вызовы и игроки.

Информационное пособие

В пособии введены понятия о кибервойне и информационной войне. Подробно освещена методика ведения информационной войны в Интернете, описаны как ее психологические, так и технические методы. Рассказано об искусственном интеллекте и его влиянии на создание кибероружия и достижение преимущества в кибервойнах.

В работе уделено внимание почерпнутым из открытых источников OSINT методам разведки в условиях ведения кибервойны или информационной войны, которая дает большие преимущества в кибероперациях. Все крупные страны уже создали свои кибервойска и доктрины ведения кибервойн. В пособии отмечены наработки в этой области таких стран, как Россия, Китай, США, Великобритании и др.

С другой стороны, должна наращиваться мощь кибероборонны. Особенное внимание необходимо уделить объектам КИИ, где важны как классические приемы ИБ, так и проактивная защита.

Пособие будет полезно специалистам, так или иначе занимающимся исследованиями в области кибервойн, студентам и аспирантам, интересующимся данной тематикой.

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

Межсетевые экраны прикладного уровня, Web Application Firewall (WAF)

En **Application Layer Firewalls, Web Application Firewall (WAF)**

A. V. Belyaev,
PhD (Eng.), Associate Professor
avb778@ya.ru

S. A. Petrenko,
PhD (Eng., Grand Doctor, Full Professor)
s.petrenko@rambler.ru

Saint-Petersburg State Electrotechnical University «LETI»

At the beginning of 2020 Information systems integration schemes using the HTTP as a transport have confidently taken a de facto leading position in applications. In fact, in the course of this process, the HTTP protocol itself has undergone significant changes, and currently has two qualitatively distinguishable functions: both direct delivery of heterogeneous content from the server to the client in an asymmetric scheme, and a practically symmetrical messaging protocol between two equal participants in information interaction. This situation has led to the emergence of a new point of possible control over the execution of computing processes, which developers of information security software systems did not fail to use, as a result of which a new technology and the corresponding class of software products appeared – application layer firewalls (L7) Web Application Firewall (WAF). Let's consider the mentioned technology and solutions in more detail.

Keywords: microservice application architecture, transport protocol, HTTP, security threat model, intruder model, application layer firewalls (L7)

В начале 2020-х годов схемы интеграции информационных систем, использующие протокол HTTP в качестве транспорта, уверенно заняли лидирующую позицию в различных приложениях. Важную роль в этом сыграли: скачкообразно выросшая доля распределенных приложений, построенных с использованием микросервисной архитектуры; стандартизация и массовое внедрение протоколов обмена прикладными сообщениями на базе форматов XML и JSON, использующими HTTP на транспортном уровне; продолжающееся увеличение уровня вычислительных ресурсов, доступных для обработки единичного сообщения (как на стороне отправителя, так и на стороне получателя), и полосы пропускания сетевой инфраструктуры. Фактически, в ходе данного процесса сам протокол HTTP претерпел серьезные изменения и в настоящее время несет две качественно различные функции: непосредственной доставки разнородного контента от сервера к клиенту в асимметричной схеме и практически симметричного протокола обмена сообщениями между двумя равноправными участниками информационного взаимодействия. Такая ситуация привела к появлению новой точки возможного контроля исполнения вычислительных процессов, которой не преминули воспользоваться разработчики программных систем защиты информации, в результате чего появились новая технология и соответствующий класс программных продуктов: межсетевые экраны прикладного уровня (L7) Web Application Firewall (WAF). В статье подробно рассмотрены как сама эта технология, так и основанные на ней решения.

Ключевые слова: микросервисная архитектура приложений, транспортный протокол, протокол HTTP, модель угроз безопасности, модель нарушителя, межсетевые экраны прикладного уровня (L7)

Андрей Владимирович Беляев,
кандидат технических наук, доцент
avb778@ya.ru

Сергей Анатольевич Петренко,
доктор технических наук, профессор
s.petrenko@rambler.ru

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Текущее состояние развития WAF

Контроль исполнения вычислительных процессов по их внешнему обмену (сетевое взаимодействие, файловая подсистема, разделяемые объекты в оперативной памяти и т. п.) возможен на различных уровнях, характеризующихся разной глубиной декодирования наблюдаемой информации [1–5, 8–10, 15–17]. Для сетевого обмена, исторически обладающего отчетливой системой уровней взаимодействия, это наиболее показательно:

- на сетевом уровне возможен контроль взаимодействующих сущностей, их локаций, характеристик частного канала обмена в глобальной информационной сети (фрагментация, приоритезация и т. п.);
- на транспортном уровне возможен анализ характеристик потока;

- на уровне представления и прикладном уровне – форматный и, частично, логический контроль сообщений.

С переходом на каждый последующий уровень количество параметров, поддающихся анализу, и сложность правил качественно возрастает, что, несомненно, сказывается на стоимости разработки и поддержки решения, но одновременно позволяет эффективно противодействовать все более широким классам несанкционированных воздействий. Предельным уровнем является контроль собственно инвариантов логики самого вычислительного процесса, однако в общем случае затраты на разработку подобной системы контроля могут сравниться с затратами на разработку защищаемого приложения и даже превосходить таковые (исключения будут приведены далее) [6, 7, 11–14].

С учетом вышеизложенного, контроль на прикладном уровне (протокол HTTP как транспорт и протоколы обмена прикладными сообщениями) расценивается экспертами в области защиты приложений как оптимальное отношение совокупной стоимости приобретения и содержания средств защиты к спектру контролируемых классов несанкционированных воздействий, что и привело к бурному развитию WAF в последние пять лет [15–17].

На рис. 1. представлены результаты анализа лучших решений класса WAF по состоянию на начало июня 2022 года.

Согласно аналитике Gartner (см. рис. 1) [13–17], среди решений класса WAF лидерами (Leaders) являются решения Akamai, Imperva, претендентами (Challengers) – CloudFlare, F5, Fastly, Amazon Web Services, Barracuda, провидцами (Visionaries) – Fortinet, Microsoft и нишевыми игроками (Niche Players) – Radware, ThreatX.

Информация о способности WAF обнаруживать некоторые наиболее распространенные классы атак и противодействовать им сведена в табл. 1.

Как следует из таблицы, наиболее прогнозируемое и успешное функционирование WAF происходит в отношении атак, в наименьшей степени связанных со спецификой конкретного приложения. Так, все лидеры рассматриваемого сегмента рынка успешно противостоят атакам из списка OWASP Top10 (2021). Данный факт, в первую очередь, свидетельствует о зрелости данного класса СЗИ. Соответственно, основная конкурентная борьба в части функциональных возможностей WAF разворачивается в отношении атак, эксплуатирующих специфичные уязвимости прикладных систем, включая:

- уязвимости используемой архитектуры;
- уязвимости распространенных сторонних библиотек и/или компонентов;
- уязвимости конкретных программных реализаций.

Исследования в области построения средств защиты информации, формирующих модель исполнения вычислительного процесса по наблюдаемому внешнему информационному обмену (модель черного и серого ящиков), велись практически с первых лет возникновения компьютерной безопасности как отрасли. Web Application Firewalls взяли на вооружение данную технологию. К тому же этап бурного развития данных СЗИ совпал с периодом качественных изменений в области алгоритмов машинного обучения (Machine Learning), что неминуемо привело к включению поведенческих алгоритмов практически во все передовые продукты класса WAF.

Применение алгоритмов машинного обучения позволило в некоторой степени преодолеть проблемную ситуацию прикладного характера, заключающуюся в том, что в условиях постоянного нарастания сложности атак и, соответственно, правил их обнаружения и противодействия им, только достаточно небольшая часть организаций-пользователей СЗИ может позволить себе иметь в штате сотрудников с очень узкой специализацией. На примере систем обнаружения вторжений (IDS), чьи функции весьма близко пересекаются с функциями WAF, это можно продемонстрировать тем фактом, что подавляющее большинство компа-

Источник: Gartner Inc.

Рис. 1. ***Лучшие решения класса WAF***
а) результаты анализа по состоянию на сентябрь 2019 года ,
б) результаты анализа по состоянию на октябрь 2020 года,
в) результаты анализа по состоянию на август 2021 года

Таблица 1. ***Противодействие WAF-атакам злоумышленников***

Класс атаки	Способность	Комментарий
Ошибки настройки доступа к ресурсам: общий случай	Нет	За исключением методов с построением поведенческого профиля
Ошибки настройки доступа к ресурсам: частные случаи, например, выход за пределы разрешенного каталога	Да	
Атаки на подсистему аутентификации, в том числе полный перебор учетных данных	Да	
Перехват сессии	Да	В случае изменения сетевых характеристик клиентской стороны
Передача вредоносного контента	Да	Обычно осуществляется с помощью внешних подключаемых модулей, например, антивирусных решений
Включение в запрос недокументированных параметров	Нет	За исключением методов с построением поведенческого профиля
Атаки на уровень представления информации (парсеры), в том числе переполнение буфера, передача умышленно больших объемов сжатой информации, зацикливание рекурсии разбора сообщения и т. п.	Да	
Инъекция команд и/или кода (в том числе SQL, JavaScript): общий случай	Частично	Для известных разновидностей атак
Инъекция команд и/или кода в параметрах вызова	Да	
Запросы, содержащие признаки атаки удаленного исполнения кода	Да	В большинстве случаев
Утечка информации в ответных сообщениях	Нет	За исключением методов с построением поведенческого профиля
Эксплуатация недокументированных возможностей, в том числе в сторонних компонентах	Частично	Для известных разновидностей атак
Атаки на отказ в обслуживании, специфичные для защищаемого приложения, например, утечки памяти, некорректные сочетания параметров	Нет	
Атаки, требующие многократного повторения запроса (автоматизированные), в том числе сканеры уязвимостей, и fuzzy-сканирование	Да	

ний, несмотря на очень гибкие возможности подсистемы построения правил, практически не формируют их самостоятельно. Наиболее часто встречаются три схемы применения.

Уже на этапе выбора продукта компания осуществляет отбор решения с максимальным предустановленным набором правил/сигнатур (при этом из-за использования различными решениями различных алгоритмов кодирования правил непосредственное количественное сравнение на самом деле непоказательно), а затем отключает часть из них по факту выявления ложных срабатываний в ходе тестирования или продуктивной эксплуатации. Здесь стоит отметить, что производители WAF, формирующие сигнатуры мелкой гранулярности, оказываются де-факто в преимущественном положении в ситуациях, когда сотрудники компании-пользователя, ответственные за управление подсистемой правил, отключают в случаях ложных срабатываний сигнатуры целиком вместо надлежащего редактирования входящих в них предикатов.

На этапе внедрения продукта приобретается предпроектное обследование защищаемых приложений, позволяющее сформировать достаточно точный фиксированный поведенческий профиль силами сотрудников внедряющей компании, обладающих достаточным уровнем компетенций. Точность сформированного профиля зависит от репрезентативности материалов (входных и выходных данных) и сценариев работы приложений, предоставленных заказчиком. Недостатком подхода является статичность набора правил/сигнатур, что начинает выражаться в постепенно ухудшающихся со временем показателях обнаружений/ложных срабатываний. Скорость этого процесса, как правило, зависит от частоты внесения изменений в само защищаемое приложение.

Заказчик приобретает обслуживание сигнатурной модели обнаружения как сервис. При очевидных наиболее высоких характеристиках качества данный подход является наиболее дорогостоящим для потребителя, а кроме того, может быть применен только при наличии на рынке организаций, предоставляющих услуги для выбранного WAF-продукта.

Во всех перечисленных выше случаях не рассматриваются обновления баз сигнатур, отражающие новые схемы атак и уязвимости, ставшие известными после внедрения продукта, что у подавляющего большинства разработчиков расценивается в качестве услуг по базовому техническому сопровождению приобретенного продукта по схеме ежегодной подписки.

Возвращаясь к качественно новому подходу решения описанной проблемы, предлагаемому машинным обучением, стоит отметить, что наличие данной технологии в неко-

тором смысле перемещает процесс формирования модели защищаемого приложения внутрь периметра компании заказчика, замещая услуги внешнего высококвалифицированного персонала и во многих случаях увеличивая скорость адаптации данной модели к изменениям в защищаемом продукте. К основным потенциальным рискам применения указанной технологии следует отнести трудно прогнозируемый уровень ложных срабатываний, а также постепенно появляющиеся исследования в области методик обхода алгоритмов машинного обучения, основанных на специфике их архитектуры.

В целом развитие методов обхода правил и моделей WAF не является чем-то специфическим только для модулей, основанных на машинном обучении. Практически одновременно с процессом становления данного класса СЗИ стал формироваться целый спектр способов вывода атакующих воздействий из-под правил обнаружения WAF. Во многом для этих целей были задействованы уже применявшиеся ранее подходы сокрытия вредоносного кода от сигнатурных антивирусов. Как и ранее, основной принцип заключается в поиске различий реализации стандартов обработки (например, декодирования уровня представления и прикладного уровня) сообщений между WAF и атакуемым приложением. Целью является преобразование вредоносного вектора таким образом, чтобы атакуемое приложение восприняло его как оригинальное (то есть произошла бы реализация целевой уязвимости), а межсетевой экран прикладного уровня в процессе обработки вектора не смог бы сформировать его ключевые атрибуты. Например, на уровне представления широко используется внедрение специальных символов, экранирование (зачастую многократное), редко используемые соглашения по кодированию символов, а также знание специфики реализации процесса декодирования конкретными библиотеками, используемыми атакуемым приложением. Данный аспект заставляет обратить внимание при выборе WAF-решения на скорость реакции производителя на сведения о новых способах обхода фильтрации, разрабатываемых злоумышленниками, а также (в случае наличия *Service Level Agreement* (SLA), то есть соглашения об уровне услуги) в части доступности защищаемого сервиса) на организацию процесса обновления экрана прикладного уровня, обеспечивающую минимальный простой продуктивной среды.

С учетом описанной выше ситуации при фактически равных базовых возможностях состоявшихся WAF-решений следует выделить следующие характеристики, которые остаются специфическими для отдельных продуктов и могут иметь ключевое влияние на их выбор в зависимости от требований к процессу защиты:

- гранулярность предустановленных сигнатур/правил;
- схема обновления сигнатур, предлагаемая производителем (а также ее стоимостная политика);
- алгоритмы обнаружения повторяющихся (автоматизированных) активностей, в том числе вероятностного (fuzzy) подбора параметров вектора атаки;
- принцип работы алгоритмов построения поведенческого профиля защищаемого приложения, в том числе:
  - схема обучения модели;
  - схема применения обученной модели к продуктивной среде;
  - возможности (гранулярность, оперативность) внесения корректив в примененную модель с целью отключения ложных срабатываний, выявленных на продуктивной среде;
- своевременность выпуска критичных обновлений продукта в случае обнаружения способов обхода фильтрации;
- возможность обновления компонентов решения с минимальным временем простоя продуктивной среды;
- схема подключения к инспектируемому потоку, в том числе схема обмена информацией (обнаружение корреляций между воздействиями) в случае защиты приложений с балансировкой сетевой нагрузки;
- возможность интеграции с внешними сервисами, в том числе:
  - антивирусными решениями;
  - системами противодействия утечкам информации (DLP);
  - репутационными сервисами;
  - системами управления событиями информационной безопасности (SIEM).

Результаты сравнения лучших решений класса WAF по аналитике Gartner, по техническим характеристикам, а также пример выбора решения класса WAF для систем дистанционного банковского обслуживания (ДБО), представлены в табл. 2–4.

Развитие отечественных WAF-решений

Сначала определим критерии сравнения и соответствующие эталонные значения технических характеристик упомянутых решений. К возможным критериям для сравнения отечественных решений WAF относятся:

- попадание вредоносного программного обеспечения через защищенный периметр;
- эксплойты нулевого дня при проходе через защищенный периметр;
- передача контента с измененным форматом файла в обход проверки подписи;
- попытка передачи «декомпрессионной бомбы».

Эталонными характеристиками являются:

- профиль трафика 10 Тбайт в сутки, максимальная нагрузка в час – 1,5–2 Тбайт;
- многопоточный режим работы: синхронный/асинхронный/псевдосинхронный;
- поддержка ICAP, SOAP, HTTPs (GraphQL, gRPC), Websocket;
- проверка в режиме реального времени: время отклика – менее 1 с, максимальный размер файла – 500 Мбайт;
- проверка в псевдореальном времени: время отклика – 1–2 с, максимальный размер файла – 2 Гбайт;
- проверка в асинхронном пакетном режиме: время отклика – 100 мс, время до получения результата проверки до 5–10 мин., максимальный размер пакета – 5 Тбайт;

Таблица 2. ***Результаты сравнения (по 5-бальной шкале) лучших решений класса WAF по аналитике Gartner***

Название / Показатель	Imperva	F5	Radware	Fortinet	Barracuda	Akamai	Cloud Flare	Amazon Web Services
Локальный или облачный	Локальный	Локальный	Локальный	Локальный	Локальный + облако	Облако	Облако	Облако
Защита от ботов	4,1	4,2	4,5	4,3	4,5	4,6	4,5	4,3
Безопасность API	4,0	4,3	4,7	4,4	4,6	4,4	4,7	4,6
Защита от известных угроз	5,0	5,0	4,4	5,0	5,0	–	4,7	4,8
Оповещение и отчетность	5,0	4,7	4,2	5,0	5,0	–	4,3	4,4
Расширенная безопасность	5,0	4,7	4,6	4,5	5,0	–	4,0	4,2
Простота использования, объем работ по обслуживанию	4,0	4,7	4,3	5,0	5,0	–	5,0	4,4
Масштабируемость – производительность	4,0	4,7	4,6	5,0	5,0	–	5,0	4,6
Интеграция	–	4,7	4,6	4,5	4,8	–	5,0	4,2

Таблица 3. ***Результаты сравнения лучших решений в классе WAF по техническим характеристикам***

Название / Показатель	Imperva	F5	Barracuda
Сниффер (Sniffer)	Да, Non-Inline Sniffer	Нет	Нет
Мост (Bridge)	Да, Transparent Bridge (Layer 2) with Fail-Open (Hardware Bypass)	Да	Да, Bridge Path
Ретроспективный анализ (анализ логов/записей трафика)	Нет	Нет	Нет
Вариации поставки	Виртуальный/аппаратный/облачный	Виртуальный/аппаратный/облачный	Виртуальный/аппаратный/облачный
Терминация/Детерминация SSL	Да/Да	Да/Нет	Да/Да
Пассивное дешифрование SSL	Да	Да	Да
Поддержка схем кластеризации Active – Active и Active – Passive	Да	Да	Да
Максимальная поддерживаемая загрузка пропускного канала (пропускная способность)	Для аппаратной платформы: 10 Гбит/с – модель X10K. Для виртуальной машины: до 1 Гбит/с – модель V4500. Для Amazon Web Services: до 500 Мбит/с – модель AV2500. Для Microsoft Azure: до 500 Мбит/с – модель MV2500	Для аппаратной платформы: - 84 Гбит/с (L4)/40 Гбит/с (L7) – модель 12250v; - 160 Гбит/с (L4)/80 Гбит/с(L7) – модель i10800. Для блейдового шасси: 140 Гбит/с (L4/L7) – модель VIPRION 4450 Blade. Для виртуальной машины: 40 Гбит/с (L4) – модель High Performance VE	Для аппаратного комплекса: 5 Гбит/с – модель 960. Для виртуальной машины: 4 Гбит/с – модель 660Vx
Максимальное поддерживаемое количество TPS/RPS	Для аппаратной платформы: 72000TPS и 9000 (RSA/Sec (2048bit)) – модель X10K	Для аппаратной платформы (SSL/TLS-транзакций в секунду): - 240 000 TPS – модель 12250v; - 48 000/84 000 TPS (ECC/RSA) – модель i10800. Для блейдового шасси (SSL-транзакций в секунду): 160 000 TPS – модель VIPRION 4450 Blade. Для виртуальной машины (SSL-транзакций в секунду): 9700 TPS (RSA) – модель High Performance VE	Для аппаратного комплекса: HTTP – 180000 TPS, SSL –50000 TPS – модель 960
Поддержка web-стандартов (помимо HTTP/HTTPS)	WebSockets, XML, JSON	WebSockets, XML, JSON	WebSockets, XML, JSON

Название / Показатель	Imperva	F5	Barracuda
Поддержка VLAN-интерфейсов	Да (для протоколов STP и RSTP)	Да	Да
Поддержка балансировки нагрузки между защищаемыми web-приложениями	Да	Да	Да
Поддержка Multitenancy	Нет	Да	Нет
Блокирование отдельного запроса	Да	Да	Да
Возможность временной блокировки запросов от источника	Да	Да (по геолокации, по IP-адресам)	Да
Реакция при блокировке	Блокирование IP-адреса атакующего, блокирование HTTP-запроса/ответа, сброс соединения (TCP Reset)	Блокирование IP-адреса атакующего	Перехват сессии, сброс TCP-соединения
Информирование пользователя с указанием уникального идентификатора запроса в случае блокировки	Да (landing page)	Да (специально сгенерированная страница с необходимой информацией для обращения в службу поддержки)	Да (Custom Response Page)
Наличие собственного исследовательского центра	Да: Центр защиты приложений Imperva (*Application Defense Center*, ADC)	Да: F5 Security Research Team	Да: Barracuda Labs охватывает широкую сеть из 150 000 сенсоров по всему миру
Наличие предустановленных правил корреляции детектирования атак	Да	Да	Да
Наличие репутационных баз (IP, URL)	Да	Да	Да
Категоризация по типу активности (типу атаки) вредоносных хостов	Да	Да	Да
Обнаружение ботов на основе: - значений полей запроса (например, поля User Agent или других полей запроса) - последовательности переходов по ресурсам web-приложения	Да	Да	Да

Таблица 4. ***Пример выбора решения класса WAF для ДБО***

Требования к решению	Imperva	F5 BIG-IP Application Security Manager	Radware AppWall
Задачи системы			
Машинное обучение, анализ угроз и глубокая экспертиза систем ДБО	Соответствует	Соответствует	Соответствует
Противодействие различным видам угроз и атак, в том числе OWASP TOP-10 (2021) и другим нарушениям информационной безопасности, связанным с работой расположенных в корпоративной среде систем ДБО, к которым открыт публичный доступ из сети Интернет	Соответствует	Соответствует	Соответствует
Защита от автоматических атак ботов и других вредоносных инструментов	Соответствует	Соответствует	Соответствует
Защита от атак BruteForce	Соответствует	Соответствует	Соответствует
Обнаружение и устранение DDoS-атак уровня приложений (L7)	Соответствует	Соответствует	Соответствует
Анализ, выявление и закрытие уязвимостей в системах ДБО, осуществляющих передачу данных через HTTP- и HTTPS-протоколы	Соответствует	Соответствует	Соответствует
Обеспечение безопасности протокола API систем ДБО	Соответствует	Соответствует	Соответствует
Возможность автоматического создания правил для защиты уязвимых мест (до их устранения) в работе приложений систем ДБО	Соответствует	Соответствует	Соответствует
Предоставление сводной информации о безопасности систем ДБО, рекомендаций по улучшению защиты	Соответствует	Соответствует	Соответствует
Соблюдение требований стандарта безопасности PCI DSS	Соответствует	Соответствует	Соответствует
Общие требования			
Реализация WAF в виде виртуального устройства, устанавливаемого на серверы виртуализации банка, размещенные в разных ЦОД (модель развертывания On-premise), либо в виде программно-аппаратных комплексов с эквивалентным набором функций и характеристик	Соответствует	Соответствует	Соответствует
Поддержка платформы виртуализации VMWare ESXi в случае, если WAF поставляется в виде виртуального устройства	Соответствует	X6520 в виде аппаратной платформы, управление в виде виртуальной платформы с поддержкой Esxi 6.7 и выше	Соответствует

Требования к решению	Imperva	F5 BIG-IP Application Security Manager	Radware AppWall
Требования к компонентам системы			
Наличие подсистемы централизованного управления и мониторинга	Соответствует	Соответствует	Соответствует
Наличие подсистемы, обеспечивающей политику безопасности по разграничению и контролю доступа к системам ДБО, включая обнаружение угроз и уязвимостей	Соответствует	Соответствует	Соответствует
Наличие подсистемы обнаружения атак, обнаружения уязвимостей и антивирусной защиты	Соответствует	Соответствует	Соответствует
Наличие подсистемы представления данных, управления событиями и подготовки отчетности	Соответствует	–	Соответствует
ПО системы предоставляет возможность установки каждого из ее компонентов (подсистем) на отдельных виртуальных и физических сетевых узлах (узле захвата трафика, узле анализа, узле БД, узле управления) для создания распределенных масштабируемых и отказоустойчивых конфигураций	Соответствует	Соответствует	Не указано
Возможность запуска нескольких модулей захвата и анализа трафика на одном физическом или виртуальном узле	Соответствует	Соответствует	Соответствует
Требования к обработке трафика			
Линейная пропускная способность и латентность в миллисекунды (чтобы не оказывать влияние на производительность ДБО)	Соответствует	Соответствует	Соответствует
Работа с HTTP- и HTTPS- (SSL)-трафиком систем ДБО	Соответствует	Соответствует	Соответствует
Возможность импорта в WAF сертификатов и пар «закрытый/открытый ключ» для защиты SSL-систем ДБО	Соответствует	Соответствует	Соответствует
WAF должен уметь терминировать и расшифровывать клиентские соединения, инспектировать трафик на предмет соответствия политикам безопасности и, в зависимости от режима, повторно его зашифровывать при соединениях с системами ДБО или балансировщиками нагрузки	Соответствует	Соответствует	Соответствует
В режимах прозрачного проксирования и пассивного мониторинга сети (предпочтительно) возможность дешифрования SSL-трафика для проверки, не терминируя или не изменяя HTTPS-соединение	Да/нет для DH-алгоритмов	Соответствует	Соответствует
Требования к поддерживаемым протоколам и форматам обмена данными			
Поддержка протоколов: - HTTP; - HTTPS (SSL/TLS, включая SSL v3, TLS v1.2); мHTTP/2 и HTTP/2 B Поддержка server push: - SOAP; - Syslog; - LDAP - Возможность распознавать и обходить сценарии блокирования протокола WebSocket	Соответствует	Соответствует	Соответствует
Требования к отказоустойчивости системы			
Возможность работы в режиме высокой доступности (High) и круглосуточного режима функционирования	Соответствует	Соответствует	Соответствует
Наличие штатных средств для аварийного переключения (Failover) между нодами с предоставлением возможности настройки сценариев переключения	Соответствует	Соответствует	Соответствует
Ноды системы, объединенные в кластер, располагаются в разных ЦОД на двух географически распределенных площадках, с включенным отказоустойчивым режимом	Соответствует	Соответствует	Соответствует
Прочие требования			
Защита приложений от уязвимостей OWASP TOP-10 2021	Соответствует	Соответствует	Соответствует
Комплексная защита программных API-интерфейсов	Соответствует	В платформе Imperva реализовано через автомат, профилирование приложений и/или импортирование API-линков из Swagger-файла в профиль через Open API	Соответствует
Возможность обнаружения: - известных вредоносных источников автоматизированных атак и атак с использованием ботнетов; - анонимных прокси; - сетей TOR; - фишинговых сайтов	Соответствует	Соответствует	Соответствует
Возможность извлечения реального IP-адреса источника из произвольного поля HTTP-заголовка	Соответствует	Соответствует	Соответствует
Пропускная способность межсетевого экрана	Более 84 Гбит/с	Более 10 Гбит/с	Более 80 Гбит/с

- поддержка типов и форматов контента (файлов): видео, текст, аудио, графика, фото, электронные таблицы;
- проверка архивов (в том числе мультиархивов), мультипакетных данных, рекурсивных архивов, различных форматов файлов, файлов в кодировке base64;
- возможность добавления модулей проверки по типу и/или формату содержимого (файл);
- возможность интеграции с системой мониторинга Prometheus в части контроля нагрузки на серверные ресурсы и прикладное программное обеспечение;
- возможность контролировать порядок проверки контента в системе, наличие проверки потокового контента (файлов), интеграция с Kafka, информирование через брокеров сообщений: Kafka, Rabbit MQ;
- наличие API для запроса статуса и результатов проверки, мониторинга;
- возможность интеграции с хранилищами объектов (S3) для проверки контента;
- возможность горизонтального масштабирования системы с учетом георезервирования.

Ниже представлены краткие описания функциональности указанных в табл. 5 отечественных WAF-решений и близких им категорий продуктов: программно-аппаратных комплексов с функциями межсетевого экрана и систем обнаружения вторжений.

Программно-аппаратный комплекс (ПАК) Dionis-NX[1] представляет собой маршрутизатор и систему обнаружения и предотвращения вторжений (поддерживает протоколы GRE, PPTP, OpenVPN). Аппаратная платформа представлена сериями: Dionis-NX 2000, Dionis-NX 3000, Dionis-NX 4000, Dionis-NX 5000, Dionis-NX 7000. Различают следующие типы комплекса: серверная платформа, сетевая платформа, модульная платформа (число сетевых портов варьируется).

К основным функциям ПАК Dionis-NX относятся:

- маршрутизация трафика: статическая, динамическая и на основе политик безопасности;
- организация криптографически защищенных VPN;
- межсетевое экранирование, контроль сессий, NAT/PAT;
- обнаружение и предотвращение вторжений;
- обеспечение высокой доступности сервисов, отказоустойчивости портов и устройств;
- управление качеством сервисов, ограничение и гарантирование полосы пропускания;
- поддержка основных средств мониторинга и диагностики.

Продукт сертифицирован ФСТЭК России и входит в реестр отечественного ПО.

Программный комплекс (ПК) «Ребус-СОВ»[2] предназначен для об-

Таблица 5. ***Результаты сравнения отечественных решений WAF и их близких аналогов***

Класс защиты	№ сертификата – Система обнаружения вторжений уровня сети	Включение в реестр Минцифры	Поддержка KVM	Соответствие требованиям (по 5-бальной шкале)
ИТ.СОВ.С2.ПЗ	**3530** – программно-аппаратный комплекс Dionis-NX	Да	Нет (ПАК)	3,0
	4394 – программный комплекс обнаружения вторжений «Ребус-СОВ»	Да	Нет (ПАК)	2,5
ИТ.СОВ.С3.ПЗ	**4268** – программный комплекс «Континент-СОВ». Версия 4	Да	Нет (ПАК)	3,5
ИТ.СОВ.С4.ПЗ	**3290** – межсетевой экран и система обнаружения вторжений «Рубикон-К»	Да	Нет (ПАК)	3,0
	4501 – программно-аппаратный комплекс ViPNet xFirewall 5	Да	Нет (ПАК)	3,0
	4389 – программное обеспечение «Система сетевой безопасности Mirada»	Да	Нет (ПАК)	2,5
	4329 – система обнаружения компьютерных атак (вторжений) VIPNet IDS 3	Да	Нет (ПАК)	3,0
	4225 – программно-аппаратный комплекс Dionis DPS	Да	Нет (ПАК)	3,5
	3813 – система обнаружения компьютерных атак «Форпост», версия 3.0, исполнение 4	Да	Да	3,0
	4066 – многофункциональный комплекс сетевой защиты Diamond VPN/FW	Да	Нет (ПАК)	3,0
	4055 – программный комплекс С-Терра СОВ. Версия 4.2	Да	Да	3,0
	4042 – программное изделие «Система обнаружения и предотвращения вторжений Positive Technologies Network Attack Discovery»	Да	Нет (ПАК)	4,0
	4027 – программное изделие Kaspersky Industrial CyberSecurity for Networks	Да	Да	3,5

[1] *https://dionis-dps.ru/?yadclid=5333660&yadordid=170284183&yclid=8814487282211880 95/.*
[2] *https://www.rebus-sov.ru/.*

наружения и блокирования вторжений со стороны внешних и внутренних нарушителей и состоит из следующих компонентов: «Консоль управления СОВ», «Сервер СОВ», «Агент СОВ», «Средство сбора данных и обнаружения вторжений», «Средство противодействия вторжениям». Функционирует под управлением операционных систем Microsoft Windows, МСВС 3.0/5.0, Astra Linux Special Edition.

К основным функциям ПК относятся:

- обнаружение вторжений на основе анализа сетевого трафика, времени (сигнатурный анализ, статистический анализ, контроль состава локальной вычислительной сети);
- обнаружение вторжений на основе сигнатурного анализа журналов аудита операционной системы и прикладного программного обеспечения;
- обнаружение вторжений на основе анализа журналов аудита «Модернизированный аппаратно-программный комплекс защиты информации (АПКЗИ «Ребус-М»[3])»;
- контроль нештатных сетевых подключений на узлах и в сети;
- оперативное отображение информации о вторжениях, обнаруженных на контролируемых станциях;
- оперативное реагирование на выявленные вторжения в ручном и автоматическом режиме;
- отображение состояния агентских станций;
- визуализация собранной статистики о вторжениях;
- централизованное управление блокированием станций и сетевого трафика;
- формирование отчетов с возможностью фильтрации выводимой информации.

Соответствует требованиям руководящих документов ФСТЭК России.

Программный комплекс (ПК) «Континент-СОВ»[4] представляет собой программную систему обнаружения и предотвращения вторжений с возможностью контроля сетевых приложений (в режиме мониторинга или «в разрыв»), которая интегрируется в сетевую инфраструктуру.

Основные функциональные возможности:

- два варианта работы: обнаружение и предотвращение сетевых атак в режиме реального времени;
- двухуровневая система анализа трафика: сигнатурный анализ (более 25 000 сигнатур в базе решающих правил) и анализ сетевых приложений;
- несколько типов контролируемых приложений: системы удаленного администрирования, системы туннелирования трафика, торренты, социальные сети, мессенджеры и др.;
- автоматическое обновление базы решающих правил с серверов «Кода Безопасности»;
- сигнатуры детектора атак, разработанные лабораторией «Кода Безопасности».

Технические характеристики программного комплекса:

- иерархическое управление: три уровня иерархии управления, делегирование прав в рамках глобальной политики безопасности, сквозной мониторинг всей инфраструктуры «Континент СОВ», взаимная аутентификация главного и подчиненных ЦУС с помощью сертификатов;
- мониторинг событий в режиме реального времени;
- ролевая модель доступа администраторов;
- высокопроизводительная система хранения и обработки событий безопасности;
- дистанционное обновление компонентов комплекса (системного программного обеспечения и базы решающих правил);
- гибкая система отчетов;
- экспорт событий безопасности во внешние системы мониторинга и управления ИБ.

Соответствует требованиям руководящих документов ФСТЭК России.

Программно-аппаратный комплекс (ПАК) «Рубикон»[5] выполняет функции межсетевого экрана, системы обнаружения вторжений и маршрутизатора. Предназначен для организации эффективной защиты периметра сетей предприятий различного масштаба в соответствии с нормативными требованиями регуляторов.

Функциональные возможности ПАК:

- web-интерфейс управления с ролевой моделью доступа;
- выполнение основных функций маршрутизации;
- наличие статической и динамической маршрутизации;
- возможность резервирования на уровне устройств (по протоколу CARP);
- возможность резервирования на уровне портов (bridge, VLAN, bonding);
- возможность резервирования на уровне каналов связи по средствам динамической маршрутизации с использованием протоколов OSPF, BGP;
- возможность построения VPN-тунелей с использованием протоколов IPSec, OpenVPN и GRE (в новой версии);
- возможность трансляции сетевых адресов;
- выполнение фильтрации сетевых пакетов в режиме маршрутизатора (при использовании в режиме L3-коммутатора) по основным заголовкам сетевых пакетов;
- выполнение фильтрации сетевых пакетов в прозрачном режиме (при использовании в режиме L2-коммутатора) по основным заголовкам сетевых пакетов (в новой версии);
- возможность фильтрации сетевых пакетов по мандатным меткам отечественных защищенных операционных систем (Astra Linux и МСВС);
- наличие системы обнаружения вторжений (СОВ);
- наличие системы предотвращения вторжений;

[3] *https://cps.tver.ru/sistemi_zashiti_informatsii/complex-zashiti-informatsii/.*
[4] *https://www.securitycode.ru/products/sov-kontinent/.*
[5] *https://npo-echelon.ru/production/65/11342/.*

- возможность анализировать средствами СОВ зеркалируемый трафик (посредством span-порта);
- возможность работы СОВ в прозрачном режиме;
- наличие HTTP-, FTP-прокси;
- возможность совместного использования HTTP-прокси с внешним антивирусом по протоколу ICAP;
- локальное и удаленное обновление базы правил СОВ;
- локальный журнал регистрации событий функционирования и безопасности;
- возможность интеграции с внешними системами анализа событий безопасности;
- широкий модельный ряд аппаратного исполнения (настольные, серверные и защищенные исполнения);
- возможность использования различных сетевых интерфейсов в разных комбинациях и количестве;
- возможность применения изделия в кузовах на колесных и гусеничных шасси.

ПАК сертифицирован ФСТЭК России и Министерством обороны Российской Федерации.

Программно-аппаратный комплекс (ПАК) ViPNet xFirewall 5[6] представляет собой шлюз безопасности, реализующий парадигму NGFW и позволяющий создавать гранулированные политики безопасности на основе учетных записей пользователей и списка приложений. Обеспечивает фильтрацию трафика на всех уровнях, антивирусную защиту и предотвращение обхода политик ИБ.

Сертифицирован ФСТЭК России по:

- «Требованиям по безопасности информации, устанавливающем уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) – по 4 уровню доверия;
- «Требованиям к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016);
- «Требованиям к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016);
- «Требованиям к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012).

Программно-аппаратный комплекс (ПАК) сетевой безопасности Mirada[7] (максимальная производительность в режиме IPS/IDS – до 40 Гбит/с) является межсетевым экраном нового поколения. Устройство реализует функции системы обнаружения вторжений, автоматического применения правил безопасности, работу с зашифрованным сетевым трафиком, проксирование сетевых соединений, антивирусную проверку файлов, передаваемых по сети. Mirada может использоваться в качестве межсетевого экрана ядра сети, пограничного фаервола, а также устройства сетевого уровня. Расширенные (по сравнению с аналогичными решениями) сетевые функции позволяют реализовывать необходимый функционал при построении топологически сложных сетей.

К основным функциям комплекса относятся:

- IEEE 802.1Q VLAN – тегирование трафика для виртуальных групп;
- IEEE 802.1p IGMP – управление мультикаст-рассылками;
- IEEE 802.1D STP – устранение петель в Ethernet-сетях;
- IEEE 802.3ad – агрегирование каналов LAG, LACP;
- Port Mirroring – зеркалирование трафика SPAN, TAP;
- QoS-приоритезация трафика;
- VRRP-кластеризация;
- статическая маршрутизация;
- динамическая маршрутизация (OSPF, PBR);
- NAT.

Программно-аппаратный комплекс (ПАК) ViPNet IDS NS[8] представляет собой сетевой сенсор обнаружения сетевых атак и вредоносного программного обеспечения в файлах, передаваемых в сетевом трафике. Предназначен для интеграции в компьютерные сети с целью повышения уровня защищенности информационных систем, центров обработки данных, рабочих станций пользователей, серверов и коммуникационного оборудования.

ПАК предлагается в следующих исполнениях:

- ViPNet IDS NS100;
- ViPNet IDS NS1000;
- ViPNet IDS NS2000;
- ViPNet IDS NS10000;
- виртуальное устройство ViPNet IDS NS VA.

Может использоваться как самостоятельный продукт, а также в составе решений ViPNet Threat Detection and Response (TDR) и совместно с решением ViPNet Channel Protection.

ПАК сертифицирован ФСТЭК России и ФСБ России.

Программно-аппаратный комплекс (ПАК) Dionis DPS[9] используется в роли маршрутизатора с криптографической защитой, межсетевого экрана и сертифицированной ФСТЭК России системы обнаружения и предотвращения вторжений. Аппаратная платформа распределена по сериям и типам: серверная платформа, сетевая платформа, модульная платформа. При этом в широких диапазонах варьируется конфигурация сетевых портов.

Функциональные возможности ПАК:

- маршрутизация трафика (Dionis-маршрутизатор): статическая, динамическая (RIP, BGP, OSPF) и на основе политик, multicast-маршрутизация на младших моделях;
- организация криптографически защищенных VPN;

[6] *https://infotecs.ru/product/vipnet-xfirewall-5.html#docs.*
[7] *https://codemaster.pro/mirada#more/.*
[8] *https://infotecs.ru/product/vipnet-ids-ns.html.*
[9] *https://dionis-dps.ru/?ysclid=l47em51j53775035184/.*

- криптошлюз для защиты передачи данных (ФСБ КС1/КС3);
- межсетевой экран Dionis (ФСТЭК МЭ2/МЭ4), контроль сессий, NAT/PAT;
- система обнаружения и предотвращения вторжений (ФСТЭК СОВ2/СОВ4);
- единый центр анализа и управления системой обнаружения и предотвращения сетевых вторжений;
- PROXY, DHCP, NTP-сервер, балансировщик нагрузки с поддержкой QoS;
- сервер удаленного защищенного доступа мобильных абонентов;
- обеспечение высокой доступности сервисов, отказоустойчивость портов и устройств;
- управление качеством сервисов, ограничение и гарантирование полосы пропускания;
- поддержка средств мониторинга и диагностики, обеспечение записи всех событий в сети и оповещение администратора.

ПАК сертифицирован ФСТЭК России.

Система обнаружения и предотвращения компьютерных атак «Форпост 3.0»[10] разработана на базе распределенной системы мониторинга и управления «Форпост-мониторинг». Сохраняет функционал СОА «Форпост» 2.0 и обладает рядом дополнительных преимуществ, таких как:

- улучшенный web-интерфейс;
- скорость обработки трафика – 10 Гбит/с;
- выявление компьютерных атак с использованием сигнатурного, эвристического методов и метода поведенческого анализа;
- возможность интеграции со всеми отечественными и мировыми SIEM-системами;
- работа в ОС Windows и Linux;
- возможность работы в виртуальных средах, в том числе создание виртуальных устройств.

Система «Форпост 3.0» сертифицирована ФСТЭК России.

Программно-аппаратный комплекс (ПАК) сетевой защиты Diamond VPN/FW[11] является UTM-решением с функциями защиты каналов передачи данных, межсетевого экранирования, обнаружения и отражения атак. База сигнатур атак МКС3 Diamond VPN/FW обновляется еженедельно в автоматическом режиме с централизованного сервера или через файл локально. При детектировании сетевой атаки происходит запись в журнале событий и сохранение PCAP-файла с сетевым трафиком для дальнейшего расследования инцидента. Поддерживается написание собственных правил. Устройство может быть установлено как в разрыв канала передачи данных, так и по Т-образной схеме через SPAN-порт.

ПАК сертифицирован ФСТЭК России.

Комплекс «С-Терра СОВ»[12] представляет собой средство защиты для обнаружения кибератак на основе анализа сигнатур в сетевом трафике.

Основные функции:

- обнаружение попыток вторжений;
- детектирование атак в защищаемой сети или ее сегментах;
- отслеживание неавторизованного доступа к документам и компонентам информационных систем;
- обнаружение вирусов, вредоносных программ, троянов, ботнетов;
- отслеживание таргетированных атак.

«С-Терра БРП» (база решающих правил) для «С-Терра СОВ» зарегистрирована Федеральной службой по интеллектуальной собственности (Роспатентом) в Реестре баз данных, что подтверждено свидетельством о государственной регистрации БД.

Прикладной межсетевой экран Positive Technologies WAF (PT WAF)[13] и ***комплекс анализа сетевого трафика Positive Technologies NAD (PT NAD)***[14].

PT WAF предназначен для обнаружения и блокирования кибератак из списка OWASP Top 10 и классификации WASC, L7 DDoS и атак нулевого дня.

PT NAD (*Network Attack Discovery*) представляет собой систему глубокого анализа сетевого трафика (NTA) для выявления атак на периметре и внутри сети. Комплекс предназначен для обнаружения активности злоумышленников в обычном и зашифрованном трафике и помощи в расследованиях. Позволяет в автоматическом режиме определять типы и роли сетевых узлов, обнаруживает атаки сканирования, флуда и DDoS и обрабатывает трафик без потерь со скоростью до 10 Гбит/с. Захватывает трафик в Linux с помощью механизма DPDK (библиотека Intel) со скоростью 10 Гбит/с. В PT NAD расширен список определяемых и разбираемых протоколов. Поддерживает SQL-протоколы передачи данных: MySQL, PostgreSQL, Transparent Network Substrate компании Oracle и Tabular Data Stream. Также определяет протоколы системы Elasticsearch и печати PostScript (с помощью последнего взаимодействуют принтеры в корпоративной сети). Общее количество детектируемых протоколов – 86.

Оба решения сертифицированы ФСТЭК России по требованиям безопасности.

Программный комплекс Kaspersky Industrial CyberSecurity for Networks[15] представляет собой программное решение для мониторинга безопасности промышленной сети. Поставляется в виде программного продукта или виртуального устройства, пассивно подключаемого к сети АСУ ТП.

Основные функции:

- пассивная идентификация и инвентаризация устройств в сети;
- телеметрический анализ технологических процессов в режиме квазиреального времени;
- обнаружение несанкционированных хостов и потоков в сети;
- предупреждения о манипуляциях в сети;

[10] *https://www.rnt.ru/ru/production/detail.php?ID=689/.*
[11] *https://tssltd.ru/products/diamond-vpn-fw/.*
[12] *https://www.s-terra.ru/products/catalog/s-terra-sov-4-2/.*
[13] *https://www.ptsecurity.com/upload/corporate/ru-ru/products/af/PT_AF-3_PB.pdf.*
[14] *https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/.*
[15] *https://ics.kaspersky.ru/products/?ysclid=l47eru9y2x526139083/.*

- проверка команд, передаваемых по промышленным протоколам;
- интеграция через API-интерфейс со сторонними системами обнаружения;
- машинное обучение для обнаружения аномалий (MLAD);
- телеметрия в режиме реального времени и обработка исторических данных (рекуррентная нейронная сеть) для обнаружения киберугроз и физических нарушений безопасности.

ПАК сертифицирован ФСТЭК России.

Заключение

В сложившейся геополитической ситуации директорам отечественных служб безопасности рекомендуется обратить внимание на лучшие российские импортозамещающие решения класса WAF:

- Positive Technologies WAF + PT NAD (*Network Attack Discovery*);
- межсетевой экран UserGate F с подсистемой обнаружения и предотвращения вторжений (сертификат ФСТЭК России, виды А, Б, Д, СОВ 4 класса);
- интеллектуальный сетевой экран для защиты web-приложений SolidWall.

Так, SolidWall представляет собой классический комплексный сетевой экран для web-приложений (рис. 2). В состав решения включены:

- модуль построения поведенческой модели защищаемого приложения на базе алгоритмов машинного обучения;
- модуль сигнатурного анализа;
- модуль обнаружения автоматизированных атак;
- модуль обнаружения атак на подсистемы идентификации, аутентификации и авторизации участников информационного обмена.

Набор его базовой функциональности содержит:

- валидацию протоколов, в том числе терминирование TLS-трафика;
- разбор данных распространенных фреймворков;
- противодействие атакам OWASP Top10;
- контроль сессий пользователей web-приложений;

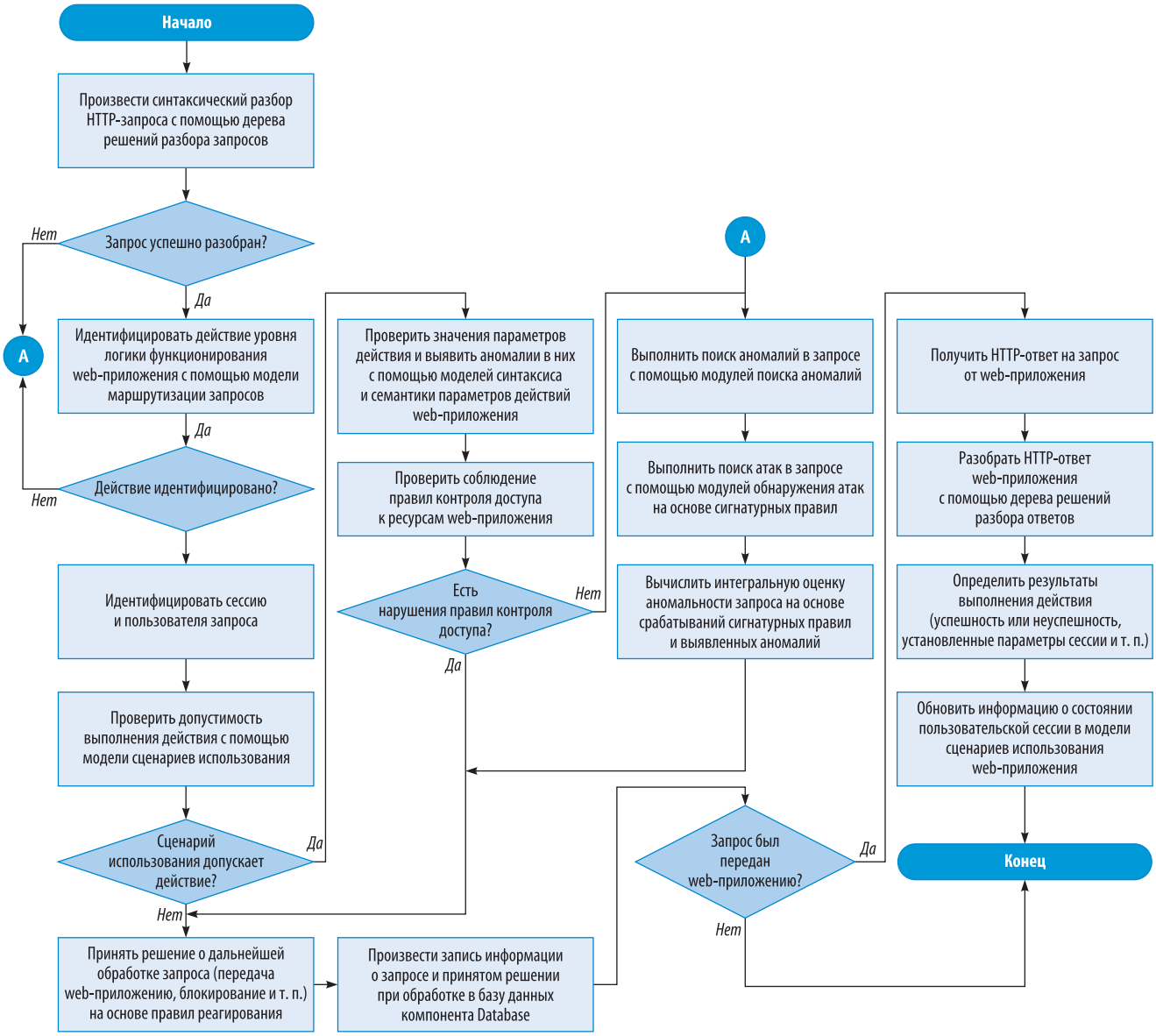


Рис. 2. ***Алгоритм работы WAF SolidWall***

- построение поведенческой модели защищаемого приложения.

На применяемые в продукте алгоритмы машинного обучения получен патент. В частности, решение осуществляет построение следующих моделей функционирования приложения:

- модель маршрутизации запросов;
- модель синтаксиса параметров вызовов web-приложения;
- модель семантики параметров вызовов web-приложения;
- модель сценариев использования web-приложения;
- модель контроля доступа к ресурсам.

Отдельный модуль решения отвечает за статистический анализ потока формируемых событий для снижения уровня ложных срабатываний и соответствующей адаптации модели верхнего уровня.

Решение поддерживает как наиболее востребованную схему подключения к информационному потоку «в разрыв» (на базе обратного прокси), так и анализ зеркалированного трафика, обеспечивая во втором варианте нулевое воздействие на передаваемые данные в процессе анализа. Узлы маршрутизации поддерживают балансировку сетевой нагрузки по схемам Active – Passive и Active – Active, а само решение позволяет осуществлять интеграцию в условиях широкого спектра масштабируемых конфигураций защищаемых приложений, в том числе с выборочной установкой модулей анализа. Несомненно, подобная гибкость архитектуры невозможна без модуля централизованного управления установленными компонентами и единого рабочего места оператора комплекса.

Среди других преимуществ продукта, традиционно востребованных в крупных внедрениях, необходимо назвать:

- поддержку версионности конфигураций каждого из имеющихся компонентов;
- возможность независимого анализа нескольких защищаемых информационных систем одной инсталляцией продукта одновременно (multitenancy);
- интеграцию с SIEM-системами.

Компания-разработчик (резидент Сколково) предоставляет услуги по предпроектному обследованию инфраструктуры заказчика, внедрению и сопровождению решения, в том числе по тонкой настройке правил и моделей, наиболее полно отражающей специфику защищаемой информационной системы. Центр компетенций компании находится на территории Российской Федерации. Интеллектуальный сетевой экран для защиты web-приложений SolidWall включен в Единый реестр отечественного программного обеспечения с декабря 2020 года. ■

Статья подготовлена по результатам исследований, выполненных при поддержке гранта РФФИ (№ 20-04-60080).

ЛИТЕРАТУРА

1. Носеевич Г. М., Гамаюнов Д. Ю., Шерварлы В. Г., Каюмов Э. М. Способ защиты web-приложений при помощи интеллектуального сетевого экрана с использованием автоматического построения моделей приложений // Патент RU (51) МПК G06F 21/00. 2013 [Электронный ресурс]. – URL: https://www.fips.ru/registers-doc-view/fips_servlet?DB=RUPAT&DocNumber=2659482&TypeFile=html (дата обращения: 15.08.2022).

2. Райс Л. Безопасность контейнеров. Фундаментальный подход к защите контейнеризированных приложений. – СПб.: Питер. – 2021. – 224 с.

3. Поллард Б. HTTP/2 в действии / пер. с анг. П. М. Бомбаковой. – М.: ДМК Пресс. – 2021. – 424 с.

4. Петренко С. А. Киберустойчивость цифровой экономики: научно-популярная монография. – СПб.: Питер. – 2021. – 384 с.

5. Петренко С. А. Киберустойчивость Индустрии 4.0: научная монография. – «Издательский Дом «Афина», 2020. – 256 с.

6. Петренко С. А., Ступин Д. Д. Национальная система раннего предупреждения о компьютерном нападении: научная монография; [под общей редакцией С. Ф. Боева]. – Иннополис, СПб: Издательский дом «Афина». – 2017. – 440 с.

7. Петренко С., Курбатов В. Политики информационной безопасности. – М.: ДМК-Пресс, Академия АйТи. – 2018. – 420 с.

8. Петренко С., Симонов С. Управление информационными рисками. – М.: ДМК-Пресс, Академия АйТи. – 2018. – 411 с.

9. Petrenko Sergei, Developing an Enterprise Continuity Program (научная монография: Разработка корпоративной программы непрерывности бизнеса // River Publishers Series in Information Science and Technology. River Publishers. 2021, ISBN: 9788770223973, e-ISBN: 9788770223966, 496 p. (Scopus).

10. Petrenko S. Developing a Cybersecurity Immune System for Industry 4.0 (научная монография: Разработка иммунной системы защиты Индустрии 4.0.) // River Publishers Series in Security and Digital Forensics. River Publishers. 2020. 386 p., ISBN: 9788770221887, e-ISBN: 9788770221870 (Scopus).

11. Petrenko S. Cyber Resilience (научная монография: Киберустойчивость Индустрии 4.0.) // River Publishers Series in Security and Digital Forensics. River Publishers. 2019. 492 p., ISBN: 978-87-7022-11-60, e-ISBN: 877-022-11-62 (Scopus).

12. Petrenko S. LA Administraciyn de la ciberseguridad. industria 4.0. (научная монография: Управление кибербезопасностью Индустрии 4.0.) // Universidad de Oviedo, Universidad de Innopolis. Oviedo, Asturias, 1st ed. 2019. 276 p. (Scopus).

13. Petrenko S. Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation (научная монография: Технологии обработки больших данных для мониторинга компьютерной безопасности) // Springer Nature Switzerland AG, part of Springer Nature, 1st ed. 2018. XXVII, 249 p., ISBN: 978-3-319-79035-0, e-ISBN: 978-3-319-79036-7 (Scopus).

14. Petrenko S. Cyber Security Innovation for the Digital Economy: A Case Study of the Russian Federation (научная монография: Инновационные технологии кибербезопасности для цифровой экономики) // River Publishers Series in Security and Digital Forensics. River Publishers. 2018, 1st ed., 490 p., ISBN: 978-87-7022-022-4, e-ISBN: 978-87-7022-021-7 (Scopus).

15. D'Hoinne J., Kaur R. etc. Magic Quadrant for Web Application and API Protection. Published 20 September 2021 – ID G00738149 // Gartner Research [Электронный ресурс]. – URL: https://www.gartner.com/doc/reprints?id=1-27HQI0PY&ct=210920&st=sb/, https://www.imperva.com/resources/resource-library/reports/magic-quadrant-for-web-application-api-protection-waap/ (дата обращения: 12.08.2022).

16. Gartner Magic Quadrant for Web Application and API Protection. Published: 20 September 2021 // Gartner Research [Электронный ресурс]. – URL: https://www.gartner.com/en/documents/4005889/ (дата обращения: 12.08.2022).

17. Web Application and API Protection Reviews and Ratings. May 2022 // Gartner Research [Электронный ресурс]. – URL: https://www.gartner.com/reviews/market/web-application-and-api-protection/ (дата обращения: 12.08.2022).

Электромагнитные поля – источник фингерпринтов

Статья посвящена обзору различных методов идентификации электронных вычислительных устройств и поиску возможных аналитических метрик. Описываются методы регистрации и анализа изменения напряженности в низкочастотных электромагнитных полях. На основе полученных данных, в ходе анализа изменения напряженности электромагнитных полей, выявляется допустимость выделения ряда характеристик, которые позволят создать уникальный фингерпринт.

Ключевые слова: идентификация, обеспечение конфиденциальности, уникальный параметр, ПЭМИН, нейронные сети, фингерпринт, электромагнитные поля, спектральный анализ

Владимир Владимирович Густов
vvg@batman.ru
Университет ИТМО

В процессе своего исторического развития человечество постоянно изобретало новые, всё более технически совершенные способы идентификации личности. Некоторые из ныне широко используемых инструментов распознавания личности человека электронными системами, такие как анализ радужной оболочки глаза, лица или голоса, еще относительно недавно считались уделом писателей-фантастов. Теперь же смартфоны умеют взаимодействовать со своими владельцами, получая от них больше данных и с большей точностью, чем в состоянии узнать о себе сами люди. Помимо того, что телефон «научился» определять своего хозяина по ряду идентификационных признаков, он «умеет» фиксировать частоту сердечных сокращений, измерять электрокардиограмму, уровень стресса, кислорода в крови и т. д.

Но можем ли мы распознавать электронные устройства так же хорошо, как они нас? Скажем, нам достаточно одного взгляда, чтобы узнать знакомого человека в толпе, или пары фраз в телефонном разговоре, чтобы распознать знакомый голос. Это происходит благодаря взаимодействию органов чувств с центральной нервной системой, и при соприкосновении человека с человеком их возможностей в большинстве случаев достаточно. А можно ли утверждать то же самое, когда речь идет об электронных устройствах? Если положить ваш мобильный телефон рядом с десятком устройств той же модели, способны ли вы отличить его от остальных? Или, если сделать backup и перенести все данные на другое устройство той же модели, заметите ли вы подмену [1]? Сможете ли вы определить, какой задаче отдаст приоритет гетерогенный планировщик вашего смартфона?

К сожалению, человек не способен воспринимать физические процессы, происходящие в электронных устройствах [2]. Следовательно, идентификация электронного устройства и получение большего количества сведений о таковом должно являться важным фактором при обеспечении конфиденциальности данных, их хранении, обработке и передаче [3, 4].

En Electromagnetic Fields are the Source of Fingerprints

V. V. Gustov
vvg@batman.ru
ITMO University

The article is devoted to the review of various methods of identification of electronic computing devices and the search for possible analytical metrics. Methods of recording and analyzing changes in intensity in low-frequency electromagnetic fields are described. Based on the data obtained, during the analysis of changes in the intensity of electromagnetic fields, the admissibility of the allocation of a number of characteristics that will create a unique fingerprint is revealed.

Keywords: identification, privacy, unique parameter, PEMIN, neural networks, fingerprint, electromagnetic fields, spectral analysis

Для создания интерфейса взаимодействия человека и электронного устройства, а также оценки физических характеристик последнего, следует воспользоваться методом регистрации и анализа изменения напряженности в низкочастотных электромагнитных полях. Каждый энергетический процесс, протекающий в каждом радиоэлементе, будет создавать сигналы, которые во множестве своем окажутся теми самыми уникальными идентификационными параметрами [5].

С целью сбора, анализа и создания базы данных измерений низкочастотных электромагнитных полей, исходящих от электронных устройств и их отдельных элементов в различных режимах работы, был спроектирован прототип детектора низкочастотных электромагнитных полей, способного регистрировать побочные электромагнитные излучения и наводки (ПЭМИН) в диапазоне до 25,6 кГц. При проектировании антенны выбор пал на катушки индуктивности за счет их способности достигать более точной локализации источника ПЭМИН [6]. В случае фиксации детектором сигнала побочного электромагнитного излучения производится его амплитудная модуляция с последующей записью в качестве аудиосигнала средствами ПК. На основе полученного аудиофайла идет построение зависимости спектральной плотности мощности сигнала от времени (рис. 1).

При накоплении базы данных появляются закономерности, которые позволяют как определять различные модули электронных устройств, так и отслеживать их режимы работы. Для удобства сравнения сонограмм произведена их структуризация по группам, на основе которой обучена нейронная сеть сверточного типа (рис. 2), что позволило добиться автоматизированного распознавания с высокой точностью типа электронного устройства на основе сигнала ПЭМИН [7, 8]. Показатель точности работы нейронной сети можно увидеть на рис. 3.

Модель нейронной сети, сформированная на основе базы из 70 трейсов с точностью от 80 до 85 %, в зависимости от таких параметров, как:

- скорость обучения;
- количество итераций;
- функция активации;
- количество скрытых слоев и единиц;
- инициализация веса;
- метод отсева,

позволила детектировать и различать различные категории электронных и электромеханических объектов, таких, как беспроводные зарядные устройства, электромеханические, на базе AVR-архитектуры, радиопередатчики, источники питания, а также комбинированные средства.

Изменяя набор обучающей базы, можно осуществлять масштабирование метода для решения с его помощью более узконаправленных задач:

- выявления определенных режимов работы электронных устройств;
- выявления попыток несанкционированного внедрения в элементную базу;
- проведения спецпроверок и специсследований;
- поиска технических средств негласного съема информации.

Резюмируя полученные данные, можно полагать, что анализ спектральной плотности низкочастотных электромагнитных полей является

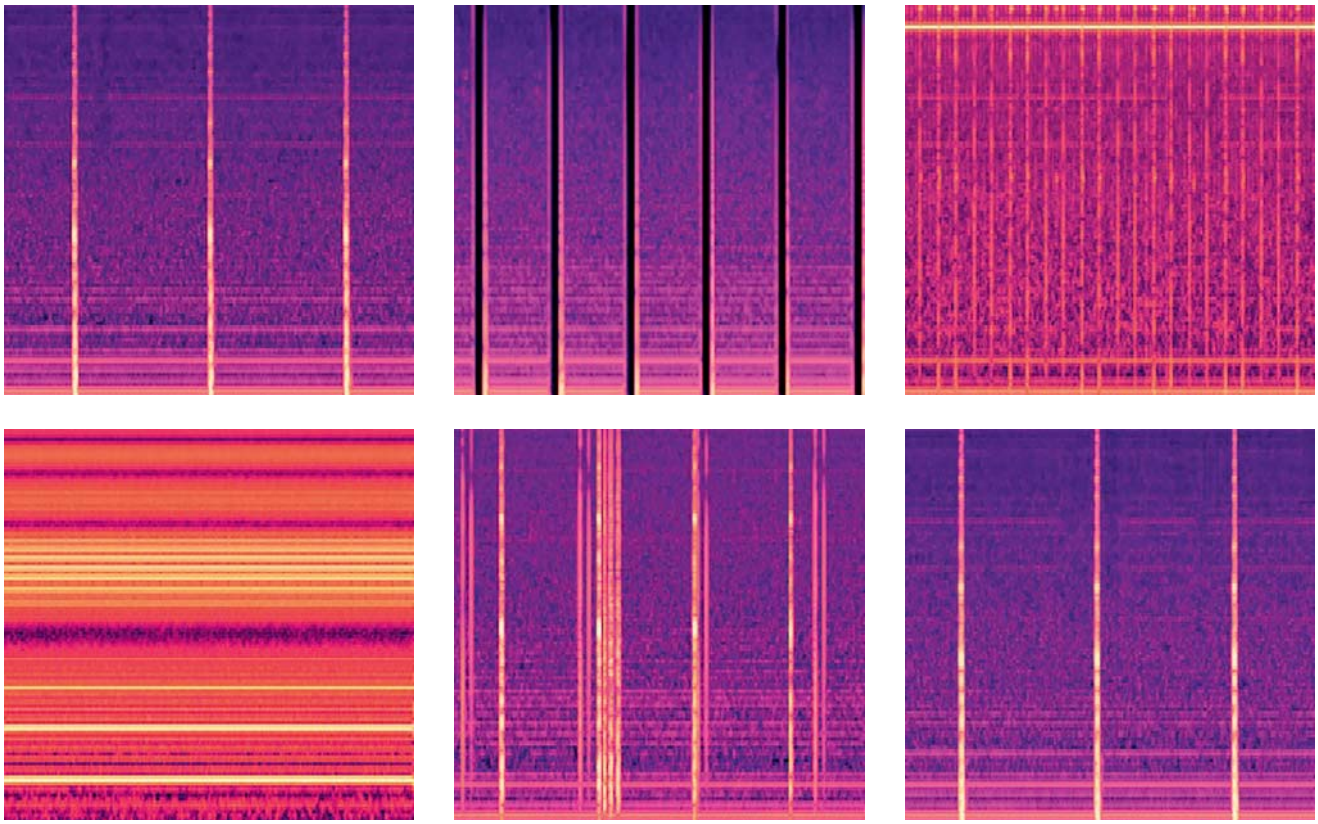


Рис. 1. ***Сравнение полученных сонограмм***

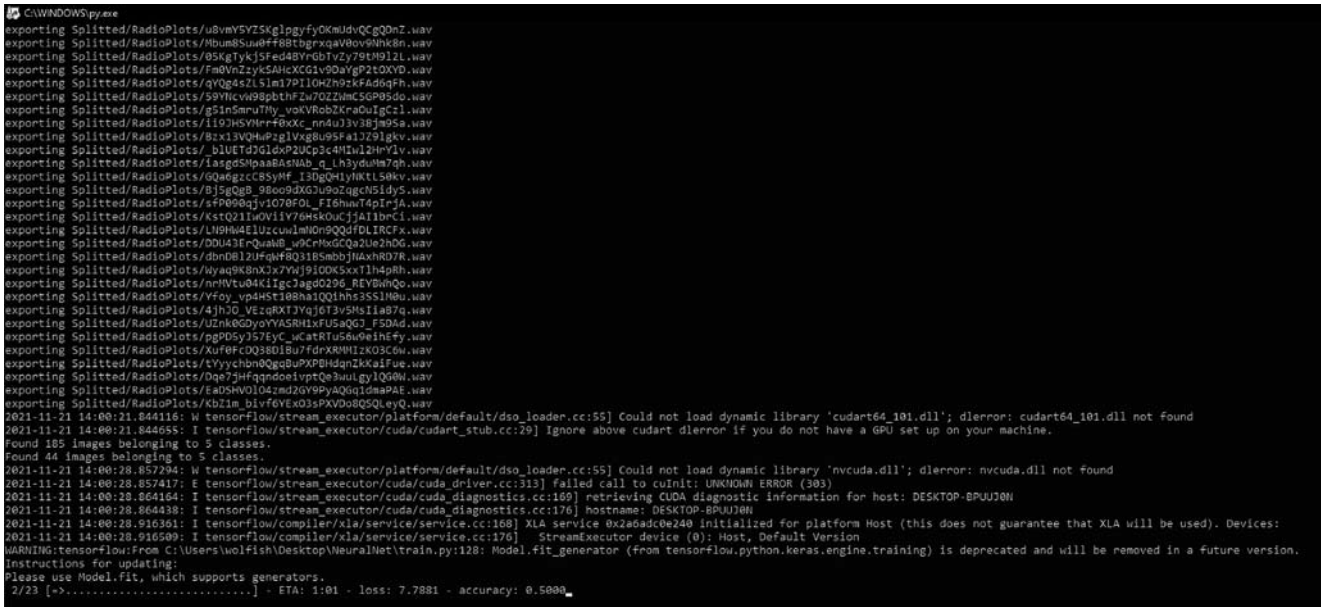


Рис. 2. ***Процесс обучения нейронной сети***

Рис. 3. ***Результат обучения нейронной сети***

подходящим методом идентификации электронных средств, генерирующих ПЭМИН.

Применение средств автоматизированного анализа многомерных данных открывает перспективу исключения ошибки оператора при выполнении сложных монотонных задач. На текущий момент времени радиочастотная разведка (Signal Intelligence) сводится, в конечном итоге, к обработке большого количества данных в отсутствие человеко-ориентированных интерфейсов взаимодействия, что указывает на потребность имплементации как систем искусственного интеллекта, так и создания userfriendly-алгоритмов визуализации массивов информации.

Такой подход позволил бы оценивать не только физические характеристики электромагнитных полей, но и вести пакетный анализ данных на более высоких логических уровнях абстракции по принципу атаки TEMPEST (*Transient ElectroMagnetic Pulse Emanation STandard*), которая представляет собой стандарт на переходные электромагнитные импульсные излучения работающей радиоэлектронной аппаратуры. Таким образом, можно было бы, например, одновременно следить за несколькими физическими показателями вычислительной техники, сравнивая выполнение задач гетерогенного планировщика. ■

ЛИТЕРАТУРА

1. Защита информации в системах мобильной связи: учеб. пособие для вузов; [под ред. А. В. Заряева и С. В. Скрыля]. – М.: Огни. – 2005. – 176 с.

2. G. Goller, G. Sigl. Side channel attacks on smartphones and embedded devices using standard radio equipment. In: Constructive Side-Channel Analysis and Secure Design – COSADE 2015, ser. LNCS. Springer. 2015. V. 9064. P. 255–270.

3. D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, Y. Yarom. ECDSA key extraction from mobile devices via nonintrusive physical side channels. In: Conference on Computer and Communications Security – CCS 2016. ACM. 2016. P. 1626–163.

4. Yan L., Guo Y., Chen X., Mei H. A study on power side channels on mobile devices. In: Symposium of Internetware – Internetware 2015. ACM. 2015. P. 30–38.

5. Густов В. В. Электромагнитные поля как признак атак по сторонним каналам // Защита информации. Инсайд. – 2020. – № 1 (91) – С. 4–7.

6. Киреева Н. В., Семенов А. В. Утечка информации по каналам ПЭМИН и способы их защиты // Международный журнал прикладных и фундаментальных исследований. – 2016. – № 8 (часть 4) – С. 499–504.

7. Хорев А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации: учеб. пособие. – М.: Гостехкомиссия РФ. – 1998. – 320 с.

8. Скоробогатов С. П. Новый способ чтения информации с памяти // ResearchGate [Электронный ресурс]. – Режим доступа: http://www.researchgate.net (дата обращения: 19.07.2022).

Разработка и программная реализация метода анализа пешеходного трафика в зоне действия Wi-Fi

En **Design and Software Implementation of a Method to Analyze Pedestrian Traffic in the Wi-Fi Coverage Area**

E. A. Basinya,
PhD (Eng.)
director@nii-ikt.ru

D. S. Khudyakov,
PhD (Eng.)
xudyakov@corp.nstu.ru

A. V. Klyuchnikova
anyyutika.ya@gmail.com

Novosibirsk State Technical University

A problem of tracking and analysis of static, pedestrian and vehicular traffic is considered in this paper. Design and software implementation of a method to analyze pedestrian traffic in the Wi-Fi coverage area, functioning according to IEEE 802.11 standards, are reviewed. The scientific novelty of the work is to propose a new method for analyzing data streams of wireless networks Wi-Fi, allowing separate accounting of devices in the network coverage area and identify abnormal network activity. Unlike existing solutions, the method allows filtering of pedestrian, static and vehicular traffic, as well as provides the ability to identify suspicious network activity due to the identification of randomized addresses and virtualization technologies.

Keywords: pedestrian traffic analysis, subscriber devices, access point, data filtering, network packets, MAC address, randomization, access control systems, Wi-Fi analytics

В работе рассматривается задача учета и анализа статического, пешеходного и автомобильного трафика. Исследуется проблематика предметной области, рассматриваются вопросы автоматизации технических процессов. На обзор выносится разработка и программная реализация метода анализа пешеходного трафика в зоне действия беспроводной сети Wi-Fi, функционирующей по стандартам IEEE 802.11. Практическая значимость предлагаемого решения заключается в возможности его использования в качестве аппаратно-программного комплекса для проведения маркетинговых исследований, а также в качестве составного модуля комплексных систем контроля доступа и безопасности предприятия, который позволит осуществлять исчерпывающий первичный сбор, анализ, обработку данных. Научная новизна работы заключается в предложении нового метода анализа информационных потоков беспроводных сетей Wi-Fi, позволяющего производить раздельный учет устройств в зоне покрытия сети и идентифицировать аномальную сетевую активность. В отличие от существующих решений метод позволяет производить фильтрацию пешеходного, статического и автомобильного трафика, а также предоставляет возможность идентифицировать подозрительную сетевую активность за счет идентификации рандомизированных адресов и технологий виртуализации.

Ключевые слова: анализ пешеходного трафика, абонентские устройства, точка доступа, беспроводные технологии передачи данных, фильтрация данных, сетевые пакеты, одноразовый MAC-адрес, рандомизация, системы контроля доступа, Wi-Fi-аналитика

Евгений Александрович Басыня,
кандидат технических наук
director@nii-ikt.ru

Дмитрий Сергеевич Худяков,
кандидат технических наук
xudyakov@corp.nstu.ru

Анна Владимировна Ключникова
anyyutika.ya@gmail.com

Новосибирский государственный технический университет

Введение

Развитие и широкое применение информационно-коммуникационных технологий (ИКТ) является глобальной тенденцией научно-технического прогресса последних десятилетий и имеет решающее значение для повышения конкурентоспособности экономики. В свою очередь, применение ИКТ позитивно влияет на ведение малого и среднего бизнеса, использующего соответствующие средства для различного рода маркетинговых исследований. Одним из вариантов подобных исследований является учет пешеходного трафика на интересуемой территории как в закрытых помещениях, так и в открытых пространствах (улицы, парки и т. д.). Для этого используются разные методы анализа, в том числе видео- и фотофиксация с распознаванием лиц, датчики входа/выхода посетителей, а также монито-

ринг публичной сети, развернутой на конкретной территории.

Обычно для исследования пешеходного трафика применяется комплекс из перечисленных ранее средств. Однако в рамках данной работы особое внимание будет уделено варианту использования публичной сети Wi-Fi.

Специально разворачиваемая общедоступная беспроводная сеть может использовать множество методов учета и идентификации посетителей, например, регистрацию пользователей по номеру телефона, что, в первую очередь, необходимо делать согласно Федеральному закону РФ № 126 «О связи». Но не все посетители будут проходить регистрацию, поэтому возникает проблема учета неавторизованных пользователей. Стоит отметить, что тема обнаружения и идентификации человека или группы людей в пространстве обсуждается не только с точки зрения полезности для ведения бизнеса, но и для обеспечения внутренней безопасности частной или государственной инфраструктуры.

Проблемой учета пешеходного трафика на базе беспроводной локальной сети Wi-Fi в настоящее время активно занимаются такие отечественные и зарубежные научные деятели, как М. В. Булыгин, H. Wang, I. B. Collings, Y. Lin, S. V. Hanly, A. Winter и др. [1–4].

Представленные исследователями методы имеют обоснованную эффективность для поставленной задачи, однако ни один из них не претендует на универсальное применение. В большинстве случаев разрабатываются методы, которые требуют внедрения дополнительных аппаратных или программных средств, в том числе со стороны пользователя [5–7]. Кроме этого, существенным недостатком является ограниченность методов относительно их применения внутри помещения и на открытых территориях без ранжирования пользователей – участников дорожного движения (пешеходов, автомобилистов) [8]. А поскольку большинство методов требует непосредственного взаимодействия клиентского устройства и точек доступа, проблема достоверности данных о MAC-адресах мобильных устройств никак не освещается и не решается. Таким образом, проблема исследования пешеходного трафика сохраняет свою актуальность и требует разработки новых методов анализа с учетом недостатков существующих решений.

Формирование концепции авторского метода для анализа пешеходного потока осуществляется на основе изучения пакетного трафика беспроводной сети, функционирующей по стандартам IEEE 802.11 (*Institute of Electrical and Electronics Engineers* – Институт инженеров электротехники и электроники). В ходе проработки решения была использована специальная функция точек доступа – сканирование радиоэфира путем перехвата сигнала от мобильных телефонов с включенным Wi-Fi-модулем проходящих поблизости людей. Радиоэфиром будем называть выделенный под негосударственные нужды диапазон радиочастот, разделяемый на каналы передачи, количество и ширина которых зависит от используемого стандарта технологии Wi-Fi. Каналы являются средой взаимодействия для базовых станций: так именуются единицы беспроводных устройств в сети. Каждая станция может быть настроена на работу в определенном частотном диапазоне и на конкретном канале или на наборе каналов с учетом синхронизации между передатчиком и приемником.

Взаимодействие между абонентским устройством и точкой доступа соответствует инфраструктурному режиму работы беспроводной сети. Данный тип сети организуется точкой доступа. После активации она инициирует процесс широковещательной рассылки сигнальных кадров (Beacon Frame), включающих в себя информацию о функциональных возможностях данной точки, поддерживаемых скоростях, политике безопасности и значении *Service Set Identifier* (SSID).

Постановка задачи

Целью данной работы выступала разработка и программная реализация метода анализа пешеходного трафика в зоне действия беспроводной сети Wi-Fi. Для достижения поставленной цели необходимо было решить следующие практические задачи:

1) исследовать структуру пакетного трафика беспроводной сети Wi-Fi с выявлением проблематики анализа данных;

2) разработать метод анализа данных трафика в зоне действия беспроводной сети Wi-Fi;

3) спроектировать общую систему анализа данных в зоне действия сети Wi-Fi;

4) программно реализовать локальный сервер для обработки HTTP-запросов от точек доступа, который будет использоваться в качестве интерфейса для взаимодействия программных и аппаратных узлов системы;

5) программно реализовать оконное приложение на базе дистрибутива операционной системы Linux для сбора, хранения данных и визуального отображения статистики.

Разработка метода

Клиентская базовая станция на начальном этапе осуществляет сканирование каналов для получения информации о доступных сетях. Указанный процесс может проходить в пассивном или активном режиме. В первом случае станция прослушивает эфир в течение определенного периода времени, ожидая появления сигнальных кадров от ближайших точек доступа. После выбора доступной сети клиент адресно на каждом частотном канале отправляет кадры пробного запроса (Probe Request) точке доступа, в которых идентифицирует себя. При активном сканировании абонентское устройство проводит широковещательную рассылку пакетов зондирования (кадров пробного запроса, Probe Request) по всем проверяемым каналам, ожидая ответов от точек доступа, получивших информацию об абоненте.

Помимо кадров пробного запроса, идентификация клиентского устройства может осуществляться на основе и кадров ассоциации (Association Request Frame), и кадров данных (Data frames), которые всегда

отправляются адресно от определенного клиента к конкретной точке доступа, но сигнал которых также могут получить любые приемники, находящиеся в зоне действия сети.

Стоит особо подчеркнуть, что сетевой пакет стандарта IEEE 802.11 имеет блок данных, предназначенный для записи физического адреса отправителя, так называемого адреса канального подуровня (*Media Access Control* – подуровень управления доступом к среде) или MAC-адреса (рис. 1). Непосредственно по нему определяется базовая станция внутри сети. Первые три байта (префикс) этого адреса являются организационно уникальным идентификатором (*Organizationally Unique Identifier*, OUI), который устанавливается производителем устройств и гарантирует глобальную уникальность адреса. Блок MAC-адресов приобретается и регистрируется в специальном органе IEEE, контролирующим все адреса с выданным трехбайтовым префиксом и несущим за них ответственность. Информация о распределении OUI находится в публичном доступе, и по ней любой желающий может определить принадлежность устройства к конкретному вендору, что потенциально влияет на появление проблемы приватности данных пользователей соответствующих технических устройств.

Заметим, что, согласно федеральному закону Российской Федерации № 152 «О персональных данных», MAC-адрес сетевого интерфейса, встроенного в мобильное устройство, не причисляется к конфиденциальным сведениям ввиду того, что он является обезличенным и лишь косвенно относится к физическому лицу, поскольку никак формально не закрепляется за конкретным человеком. Вследствие этого деятельность, направленная на сбор, хранение и обработку данных MAC-адресов абонентских устройств на территории Российской Федерации, не нарушает политики безопасности и прав граждан и может проводиться без их согласия.

В западных странах, включая некоторые североамериканские государства, тема конфиденциальности и личного пространства человека считается приоритетной при разработке ИКТ. С учетом данного факта, разработчиками популярных операционных систем, на базе которых функционирует большинство абонентских беспроводных устройств, в том числе мобильных телефонов, внедряется и по сей день улучшается система генерации одноразовых MAC-адресов, заменяющая в отправляемых сетевых пакетах назначенные производителем адреса на фиктивные. При этом существуют разные варианты реализации генерирования данных адресов и сценарии их использования.

В официальной формулировке стандартов IEEE 802.11 говорится о том, что сетевой интерфейс Wi-Fi-адаптера может либо иметь глобальный физический адрес, являющийся в обязательном порядке уникальным, либо получать локально администрируемый MAC-адрес, который не должен повторяться в своей подсети. Таким образом, генерация MAC-адресов формально не запрещена. Важно отметить, что добросовестные разработчики создают систему рандомизации физических адресов, не нарушая указаний стандартов, в первую очередь, поэтому одноразовые адреса оказываются локальными. В исключительных случаях могут быть выявлены глобальные фиктивные адреса канального подуровня, что будет являться прямым нарушением стандартов Wi-Fi. Иные принципы генерирования MAC-адресов доподлинно неизвестны, поскольку в противном случае данный механизм не имел бы практического смысла. Однако не исключено, что одноразовые MAC-адреса могут быть получены при установке в настоящем адресе специфического бита – бита локального администрирования (LA, *Locally Administered address bit*) или при использовании нераспределенных OUI с выбором абсолютно случайных чисел для *Network Interface Card* (NIC), или при выборе случайного адреса из заранее сформированного диапазона адресов.

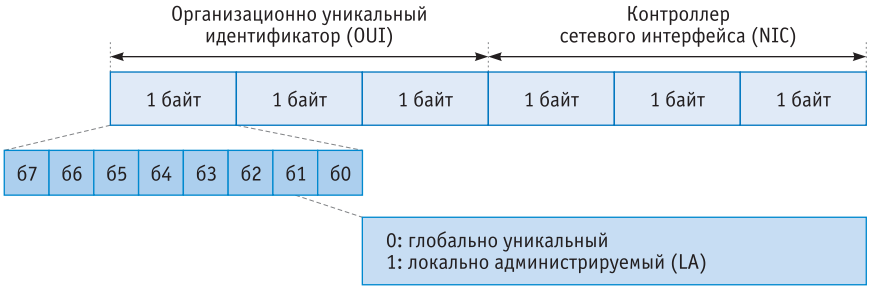


Рис. 1. ***Формат MAC-адреса***

С точки зрения исследователей, занимающихся оценкой характеристик пешеходного трафика посредством анализа кадров беспроводной сети, сценарии использования сгенерированных MAC-адресов можно классифицировать по увеличению уровня сложности выявления достоверных данных.

Самый простой вариант применения механизма рандомизации MAC-адресов заключается в замене настоящего адреса мобильного устройства при активном сканировании в кадрах пробного запроса на одноразовый до тех пор, пока пользователь не выберет подходящую сеть и не начнет адресно отправлять Probe Request или не получит ответный пакет (Probe Response) с разрешением на подключение к соответствующей точке доступа. На следующем этапе клиент отправит либо повторный Probe Request, либо пакет ассоциации уже со своим настоящим физическим адресом и идентифицирует себя в сети. Вычислить такого клиента можно при отслеживании порядковых номеров кадров: не все системы сбрасывают счетчик пакетов, что позволяет легко сопоставить снятые кадры зондирования с опознанным мобильным устройством. При условии, что счетчик пакетов был сброшен, факт присутствия пешехода в месте функционирования точки доступа однозначно будет зафиксирован.

Стоит заметить, что термин «*одноразовый адрес*» был использован здесь не случайно. Дело в том, что

при рассылке кадров пробного запроса каждый раз может генерироваться новый адрес отправителя. Следовательно, в сети будет обнаружено *n*-е количество различных адресов, принадлежащих только одному устройству. Если вести подсчет интенсивности пешеходного трафика, игнорируя данный факт, то на выходе можно получить абсолютно неправдоподобную оценку.

Более сложным сценарием работы генерирования физических адресов является смена данного адреса в кадрах, отправляемых мобильным устройством точке доступа до того времени, пока оно не пройдет все этапы подключения к сети и будет полностью авторизовано. В этой ситуации, как и в предыдущей, большую роль будут играть кадры данных, которые появятся в эфире при необходимости инициирования процесса передачи и приема информации между устройствами. Если базовая станция пользователя настроена на режим энергосбережения, то ее пакетный трафик с точкой доступа будет минимизирован. Для текущего исследования данный сценарий усложняет работу тем, что в условиях пешеходного трафика случаев полного подключения клиента к сети будет крайне мало, следовательно, уменьшается вероятность выявления действительного количества людей в зоне действия Wi-Fi.

Последней и наиболее сложной схемой внедрения системы одноразовых физических адресов является полноценное применение случайного MAC-адреса на всех этапах взаимодействия мобильного устройства с точкой доступа. В данном случае абонентское устройство никогда не выдает своего настоящего физического адреса. Кроме того, сгенерированный адрес может изменяться через определенный период времени, например, раз в день или при каждом новом подключении. Если главной задачей анализа пешеходного трафика будет являться сбор MAC-адресов целевой аудитории потребителей для последующего таргетирования рекламы, то приведенный ранее функционал окажется весомой проблемой исследования. С другой стороны, даже от ложного адреса можно получить пользу, в частности, при оценке посещаемости заведения, поскольку он будет использоваться устройством на протяжении какого-то времени в области видимости точки доступа, а значит, можно утверждать о присутствии человека на данной территории.

Уточним, что описанная логика обнаружения субъекта в пространстве имеет место быть при получении пакетов данных любого подтипа с соответствующим рандомизированным MAC-адресом в период анализа сетевого трафика. Данное условие исходит из особенности принципов взаимодействия беспроводных устройств по стандартам технологии Wi-Fi.

На текущий момент успели себя зарекомендовать несколько методов выявления реальных физических адресов клиентских устройств. В сущности, эти методы являются атаками, основанными на ряде известных уязвимостей с достаточно высокими показателями результативности. В качестве примера приведем метод атаки кармы (Karma Attack), основанный на схеме атаки «Человек посередине». Метод рассчитан на работу типового функционала клиентских устройств: при однократном подключении мобильный телефон может запомнить используемую сеть и сделать ее предпочтительной во время очередного выбора доступных сетей. Принцип действия заключается в установке ложной точки доступа с популярным публичным SSID, к которой «жертва» может подключаться автоматически и выдать необходимую информацию. Как утверждалось ранее, абонентская станция, реализующая рандомизацию MAC-адресов, использует свой настоящий адрес для подключения, начиная с этапа ассоциации. Таким образом, посредством атаки кармы злоумышленники способны быстро собирать необходимую базу данных о пользователях внутри ложной беспроводной сети.

Примем во внимание то, что в задачи настоящей работы не входила разработка метода, основанного на каком-либо роде атак мобильных устройств. Действия созданной системы по авторскому методу будут ограничиваться пассивным сканированием сети на предмет появления в эфире кадров, рассылаемых пользовательскими устройствами. Иными словами, система будет выступать в качестве наблюдателя. Вместе с тем, в момент включения режима прослушивания радиоэфира предусмотрена полная остановка приложений точки доступа, отвечающих за услуги Wi-Fi.

Предполагается, что стандартным применением авторского метода (рис. 2) будет являться анализ и фильтрация данных, полученных при сканировании Wi-Fi-сети из заголовков сетевых пакетов второго уровня OSI (*The Open Systems Interconnection model* – Модель взаимосвязи открытых систем). На входе метод, главным образом, должен получить связку «ключ – значение», где ключом выступает MAC-адрес отправителя пакетов, а значением – типы принятых кадров. На выходе с помощью метода будет сформирована база MAC-адресов с определенным статусом достоверности и соответствующим устройству производителем, а все не подлежащие анализу значения адресов будут отброшены.

Авторский метод разрабатывался с учетом выявленных особенностей формирования одноразовых MAC-адресов и принципов применения их на практике в операционных системах. Принимая во внимание тот факт, что наибольшая часть рандомизированных адресов относится к локально назначенным, начальный этап метода посвящен разделению глобально уникальных и локальных MAC-адресов.

Далее происходит проверка по типам принятых кадров: за основу берется идея, что кадры данных подтверждают факт присутствия материального устройства в сети.

Для глобально уникального адреса (без установленного бита LA) проводится идентификация производителя, за которым официально закреплен этот диапазон. Если вендор не будет найден или выяснится, что он не специализируется на производстве мобильных устройств, адрес считается фиктивным или подозрительным. При успешном определении производителя анализируе-

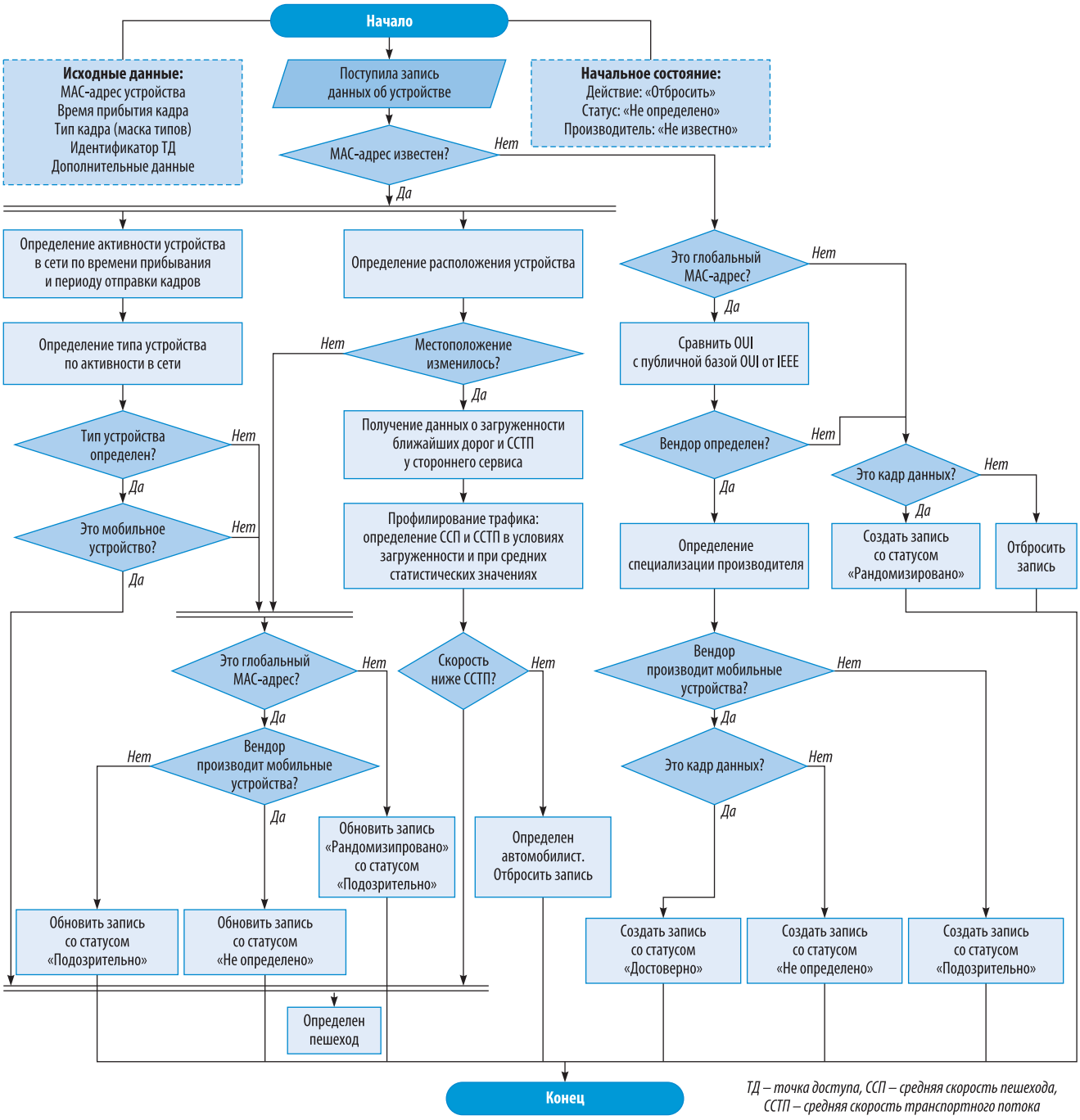


Рис. 2. ***Схема метода анализа данных***

мому MAC-адресу будет присвоен один из возможных статусов, устанавливающийся по результатам проверки типов кадров.

Кроме этого, неоднократное появление MAC-адреса в зоне действия сети позволит методу определить тип устройства по поведению и ранжировать пользователя соответствующего устройства как участника дорожного движения (пешеход, автомобилист) с помощью данных сторонних сервисов (например, Яндекс.Карты).

Таким образом, теоретически рассматриваемый метод способен улучшить положение дел при исследовании пешеходного трафика в условиях повсеместного использования одноразовых адресов, поскольку он призван исключать из исходных данных фиктивные значения, мешающие правильной оценке обстановки на рассматриваемой территории и формированию приближенных к действительности показателей статистического анализа проходящего потока людей.

Программная реализация метода

Согласно одной из поставленных целей, данная работа включает программную реализацию информационной системы, построенной на основе авторского метода анализа пешеходного трафика в сети Wi-Fi. В сущности, указанный программный продукт относится к категории программ перехвата и анализа трафика, именуемых снифферами, но в дополнение система способна со-

бирать базу полезной информации об устройствах внутри сети. Вследствие этого программа может служить средством для ведения Wi-Fi-аналитики.

Wi-Fi-аналитика – это недорогое решение, предназначенное, в частности, для маркетинговых исследований, которое позволяет получать уникальные аналитические данные о потребительской аудитории посредством наблюдений за действиями клиентов беспроводной сети. Для этого рассчитывается ряд метрик: коэффициент вхождения (entry rate), частотность посещений, среднее время нахождения в заведении, маршруты перемещений посетителей.

Обратим внимание на один немаловажный факт. В идеальных условиях Wi-Fi-аналитика должна опираться на данные от мобильных пользовательских устройств: мобильных телефонов, планшетных компьютеров или ноутбуков. При этом современный рынок цифровой техники предлагает широкий выбор, в частности, устройств Интернета вещей (*Internet of Things*, IoT), оснащенных встроенными Wi-Fi-модулями для взаимодействия друг с другом или с внешней средой. Учитывая, что радиоэфир является разделяемой средой, в реальных условиях из него необходимо выделять пакетный трафик общающихся между собой IoT-устройств, который зашумляет данные статистических исследований в период оценки пешеходного трафика.

В этой связи стоит указать границу работы авторского метода и построенной по нему информационной системы: *при сборе данных метод не может гарантировать точное определение типа устройств, видимых в зоне действия сети Wi-Fi*. В первую очередь, это связано с тем, что используемые для изучения MAC-адрес и стандартный сетевой пакет не подразделяются по типам устройств и не несут уникальную для их определения информацию. Следовательно, в базу могут входить MAC-адреса, принадлежащие в том числе IoT-устройствам, из-за чего образуется некоторая погрешность вычислений. Однако метод предусматривает определение типа устройства по поведению. Для этого ведется отслеживание перемещений устройства и скорость передвижения, а также его активность в сети.

Повышение эффективности метода может быть достигнуто интеграцией с авторской системой децентрализованного реестра событий информационной инфраструктуры предприятия и модулем интеллектуальной поддержки при принятии технических решений [9, 10].

Общая схема развертывания информационной системы (рис. 3) состоит из нескольких модулей.

«*Сервер*» – персональный компьютер администратора на базе операционной системы Linux. На него должно быть установлено нативное приложение и база данных, которая будет взаимодействовать с приложением посредством специальной программной библиотеки.

«*Коммутатор*» – аппаратный узел, служащий для подключения к серверу сканирующих точек доступа. В случае, если на сервере будет физически установлено достаточное количество сетевых интерфейсов, этот узел может быть исключен из структуры.

«*Сенсор*» – аппаратный узел, являющийся точкой доступа, работающей в режиме сканирования радиоэфира.

«*Станция*» – аппаратный узел, представляющий собой мобильную станцию пользователя с установленным Wi-Fi-модулем.

На стороне сервера для накопления, анализа и визуального отображения данных устанавливается оконное приложение. Технологический процесс работы приложения (рис. 4) разделяется на четыре подпроцесса, которые обособлены друг от друга, но связаны с помощью очереди сообщений.

Подпроцесс *Main* («Главный») отвечает за инициализацию и запуск других подпроцессов, контролируя их выполнение и завершение работы системы.

Подпроцесс *HTTP-Server* является интерфейсом для соединения точек доступа с серверной частью приложения и организует передачу принятых данных анализатору.

Подпроцесс обработки данных *Analyzer* реализует логику работы авторского метода. В функции этой части программы также входит обмен данными с модулем визуализации, работа с базой данных и сторонними сервисами.

Подпроцесс *GUI* – модуль графического интерфейса для построения визуального ряда статистики.

Для программной реализации прикладного приложения был использован высокоуровневый язык

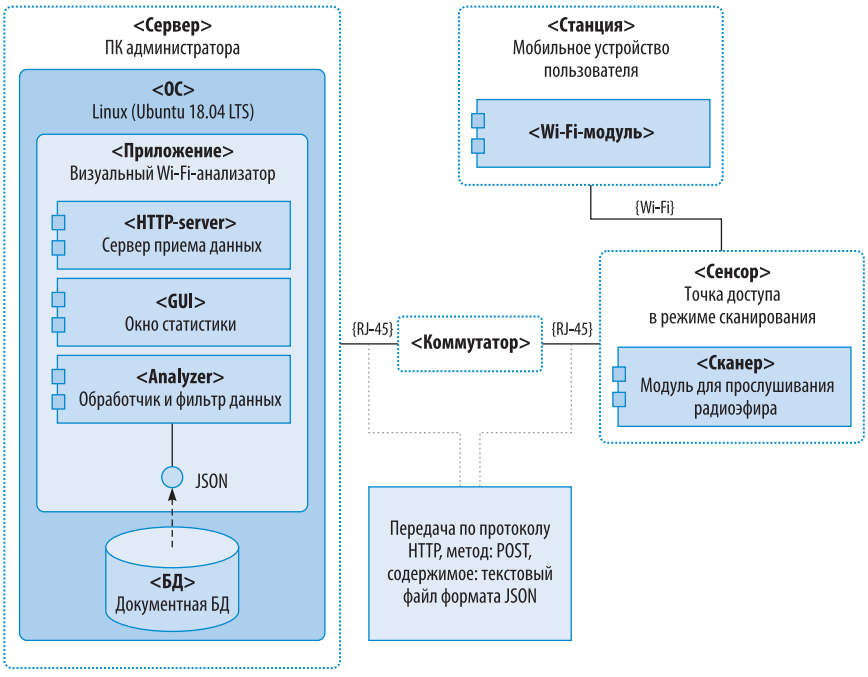


Рис. 3. ***Диаграмма развертывания проектируемой системы***

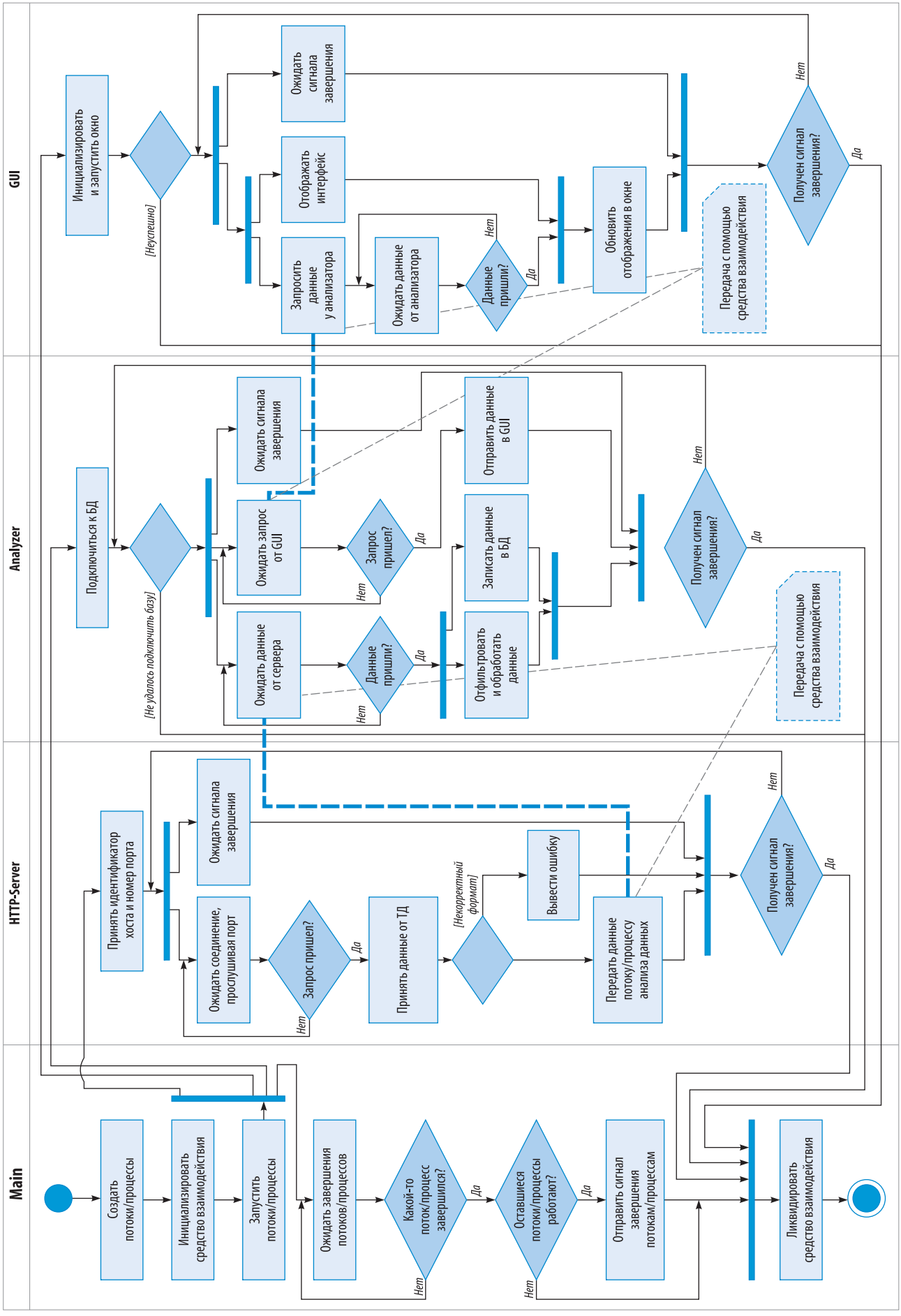


Рис. 4. Диаграмма деятельности прикладного приложения

программирования Python с рядом дополнительных инструментов.

- *Графическая библиотека Tkinter.* Это стандартный интерфейс Python для оконного инструментария Tk GUI. Пакет имеет легкие методы построения графического интерфейса. Из минусов можно отметить несколько устаревший внешний вид графических элементов, однако подобная примитивность лучше подходит для небольших настольных проектов.
- *Библиотека визуализации данных Matplotlib.* Библиотека совместима с основными пользовательскими операционными системами и графическими процессорами, вместе с тем она обладает мощным кроссплатформенным инструментарием. К недостаткам библиотеки относится отсутствие удобного способа построения более презентабельных графиков.
- *Пакет упаковки кода в исполняемый файл PyInstaller.* Python является интерпретируемым языком, поэтому существует необходимость сборки скриптов в исполняемый файл с целью скрытия исходного кода и удобного распространения ПО среди пользователей. К основным преимуществам данного пакета относятся прозрачное сжатие, способствующее формированию небольших по размеру исполняемых файлов, мультиплатформенность и поддержка динамических библиотек, обеспечивающих полную совместимость. Недостатком пакета можно назвать отсутствие поддержки кросскомпиляции.

Стоит отметить, что разработка программного продукта велась в соответствии с комплексными методологиями по организации и сопровождению технологического конвейера по разработке программных и аппаратно-программных продуктов DevSecOps. Отдельно стоит рассмотреть подходы к обеспечению качества выпускаемого программного обеспечения.

Тестирование и исследование предложенного решения

Существует множество методов тестирования программного обеспечения, с помощью которых можно убедиться, что создаваемый продукт и вносимые в его исходный код изменения будут работать, как ожидалось. Для проверки созданного прототипа были выполнены как ручные, так и автоматические виды испытаний, в частности, модульные, интеграционные, функциональные и нагрузочные тесты. По итогам проверок прототип показал положительный результат и может быть признан как MVP (*Minimum Viable Product* – минимально жизнеспособный продукт). В качестве небольшого примера приведем результаты юнит-теста для проверки анализатора данных, являющегося ядром системы (рис. 5).

Проверка функций модуля была разделена логически по разным файлам, и для каждой выделено ожидаемое поведение. По итогам тест дал положительный результат: функции отвечают поставленным требованиям.

Разработанный MVP проходил проверку производительности на специально отведенной территории предприятия, поэтому приведенные в настоящей работе изображения содержат графики и таблицы с реальными значениями.

Структура нативного приложения состоит из двух вкладок с разными видами исследований и представления данных. Стартовая страница (рис. 6) отражает информацию о состоянии системы и сети, в том числе о подключенных к системе точках доступа, предоставляющих данные для исследований.

Показанный в примере (рис. 6*г*) график демонстрирует активность пользователей в сети Wi-Fi для каждой из двух точек доступа. Полученные результаты отражают основное поведение сотрудников предприятия: прибытие на рабочее место в девять часов утра и дальнейшее пребывание на нем до шести часов вечера. Заметим, что после ухода сотрудников на территории остается примерно пятнадцать устройств, всегда присутствующих в сети. При продолжительном исследовании можно выявить точное число устройств, не относящихся к личным мобильным устройствам сотрудников, и вычитать этот показатель из статистики.

При исследовании в течение одного часа частотной метрики (рис. 7*а*), предоставляемой созданной программой, замечено, что около двадцати пяти устройств постоянно находились в области видимости точек доступа, тогда как новых было обнаружено крайне мало. Данный результат свидетельствует о том, что на этаже нет интенсивного потока людей, и присутствуют в основном постоянные работники.

Полная база данных собранных MAC-адресов отображается в виде таблицы на второй странице приложения (рис. 8). Для наглядности каждая строка с информацией об адресе окрашена соответствующим его статусу цветом.

Таким образом, в ходе программной реализации был получен рабочий вариант программного обеспечения в виде прикладного приложения, работающего на базе дистрибутива операционной системы Linux. С помощью созданной программы проверялась практическая обоснованность описанного метода и его результативность в реальных условиях.

```
============================= test session starts ==============================
platform linux2 -- Python 2.7.17, pytest-4.6.11, py-1.11.0, pluggy-0.13.1
rootdir: /home/ /radmac/test
collected 343 items
test_check_vendor_info.py ....................................... [ 14%]
test_fake_filter.py ............................................. [ 21%]
test_groupby_channel.py ......................................... [ 33%]
test_init.py .................................................... [ 38%]
test_main.py .................................................... [ 46%]
test_monitoring_trafftc.py ...................................... [ 53%]
test_msg_parser.py .............................................. [ 63%]
test_person_counter.py .......................................... [ 92%]
test_set_status.py .............................................. [100%]

========================== 343 passed in 201.46 seconds ====================
```

Рис. 5. ***Результат модульных тестов для функций анализатора данных***

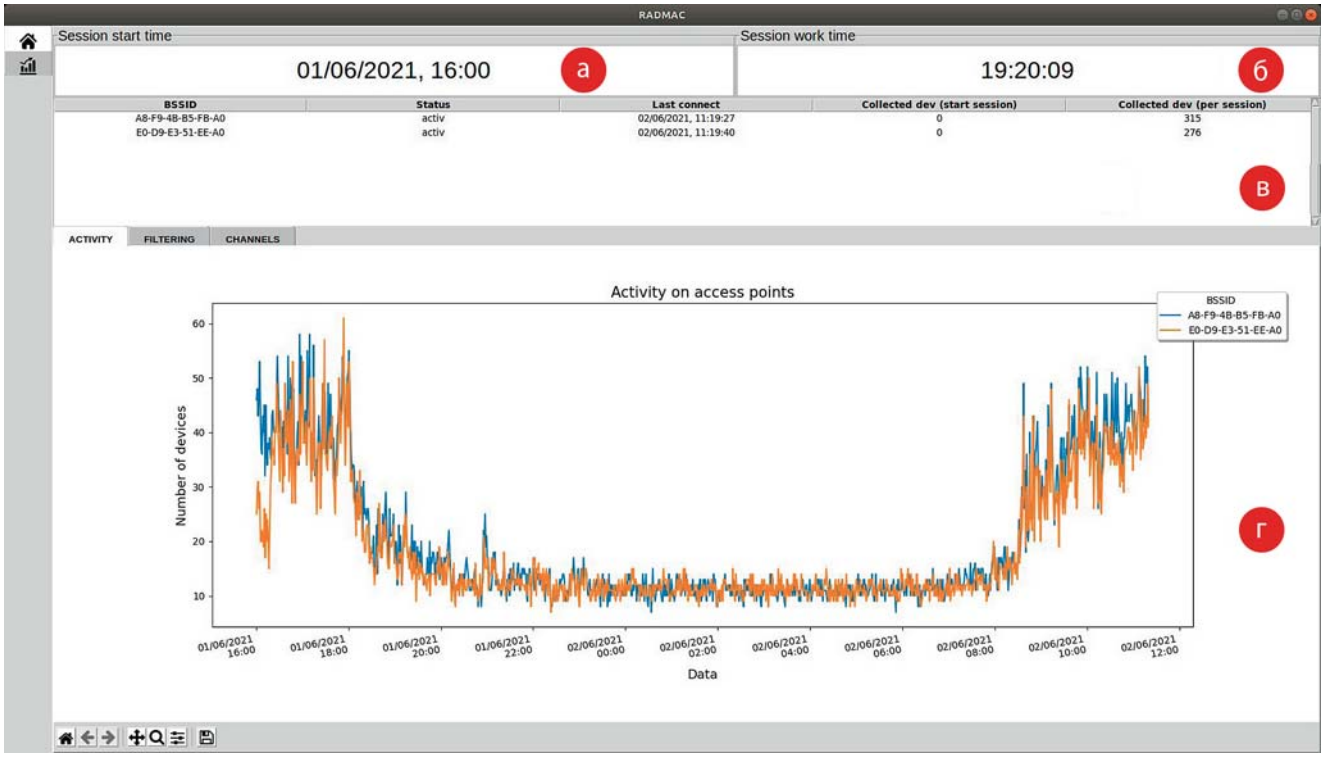


Рис. 6. ***Главная страница: а – информация о времени начала работы приложения, б – информация о периоде работы приложения в текущей сессии, в – таблица подключенных точек доступа, г – вкладки с диаграммами визуализации данных***

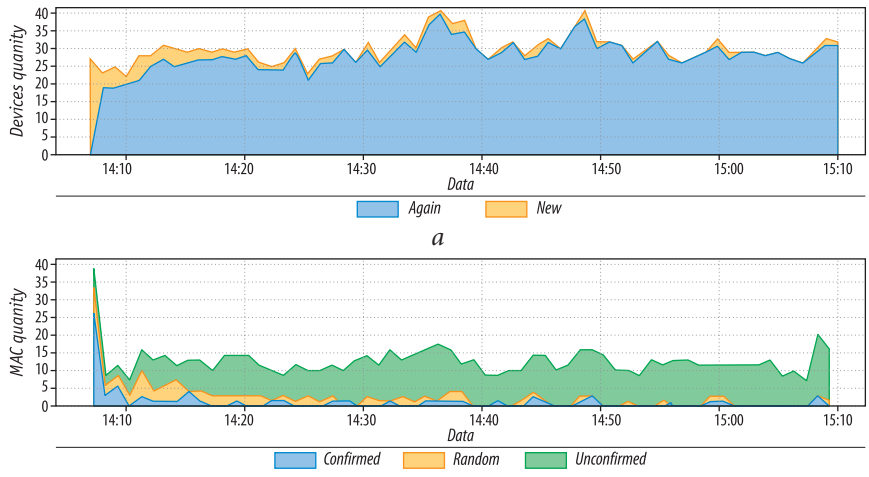


Рис. 7. ***Диаграммы анализа данных: а – статистика появления новых и повторяющихся устройств в зоне действия точки доступа, б – статистика появления разных типов MAC-адресов***

Обсуждение результатов и заключение

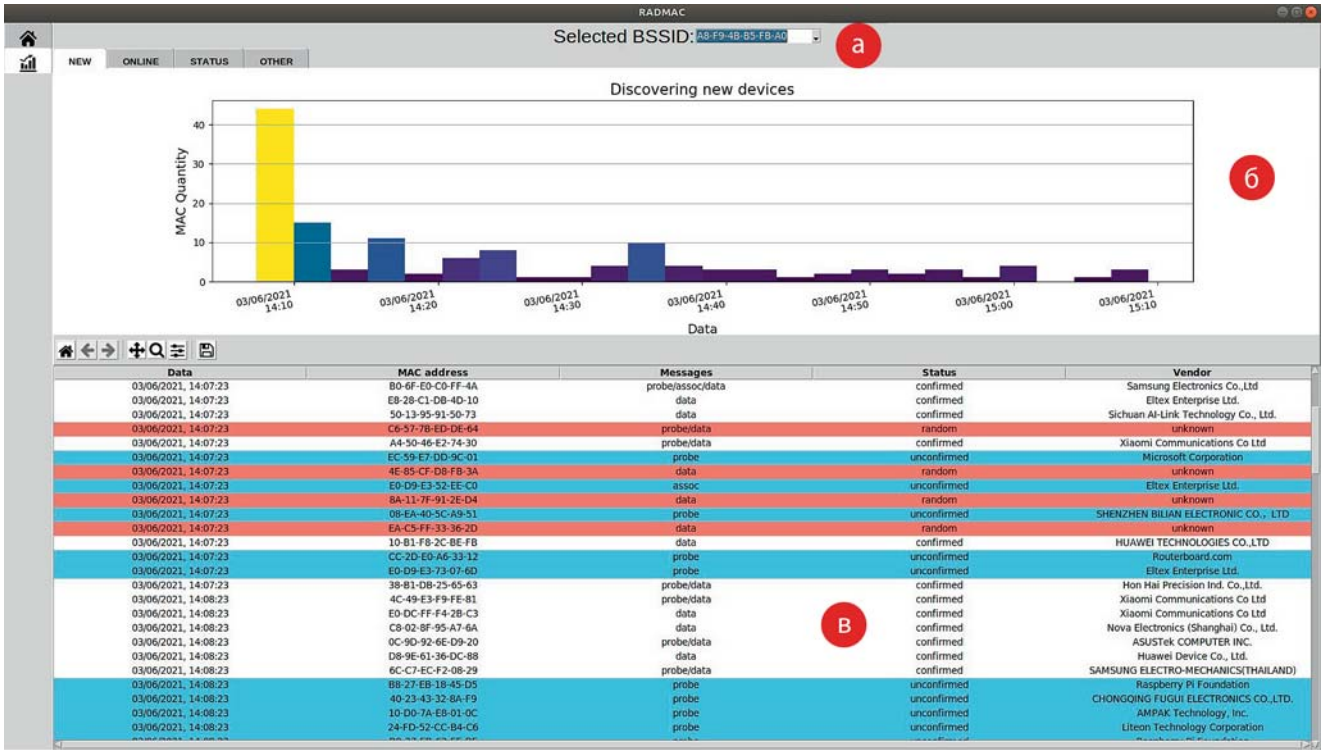
В рамках проведенной работы была поставлена цель разработать и программно реализовать метод анализа пешеходного трафика в зоне действия Wi-Fi. Для ее осуществления выполнен ряд практических задач:

- исследована структура пакетного трафика беспроводной сети Wi-Fi и выявлена проблематика анализа данных;
- разработан метод анализа данных трафика в зоне действия беспроводной сети Wi-Fi;
- спроектирована общая система анализа данных в зоне действия сети Wi-Fi;
- программно реализован локальный сервер для обработки HTTP-запросов от точек доступа, который используется в качестве интерфейса для взаимодействия программных и аппаратных узлов системы;
- программно реализовано оконное приложение на базе дистрибутива операционной системы Linux для сбора, хранения данных и визуального отображения статистики.

Вследствие этого считаем, что поставленная ранее цель достигнута и все сопутствующие задачи выполнены в полном объеме.

Актуальность работы связана с потребностью в удовлетворении спроса на статистические данные о пешеходных передвижениях, начиная от организации городской инфраструктуры по системе «Умный город» и заканчивая государственными нуждами в обеспечении внутренней безопасности. В частности, информация о пешеходных потоках полезна при маркетинговых исследованиях и принятии решений для ведения малого бизнеса.

Преимущество авторского метода заключается в предложении



Data	MAC address	Messages	Status	Vendor
03/06/2021, 14:07:23	B0-6F-E0-C0-FF-4A	probe/assoc/data	confirmed	Samsung Electronics Co.,Ltd
03/06/2021, 14:07:23	E8-28-C1-DB-4D-10	data	confirmed	Eltex Enterprise Ltd.
03/06/2021, 14:07:23	50-13-95-91-50-73	data	confirmed	Sichuan AI-Link Technology Co., Ltd.
03/06/2021, 14:07:23	C6-57-7B-ED-DE-64	probe/data	random	unknown
03/06/2021, 14:07:23	A4-50-46-E2-74-30	probe/data	confirmed	Xiaomi Communications Co Ltd
03/06/2021, 14:07:23	EC-59-E7-DD-9C-01	probe	unconfirmed	Microsoft Corporation
03/06/2021, 14:07:23	4E-85-CF-D8-FB-3A	data	random	unknown
03/06/2021, 14:07:23	E0-D9-E3-52-EE-C0	assoc	unconfirmed	Eltex Enterprise Ltd.
03/06/2021, 14:07:23	8A-11-7F-91-2E-D4	data	random	unknown
03/06/2021, 14:07:23	08-EA-40-5C-A9-51	probe	unconfirmed	SHENZHEN BILIAN ELECTRONIC CO., LTD
03/06/2021, 14:07:23	EA-C5-FF-33-36-2D	data	random	unknown
03/06/2021, 14:07:23	10-B1-F8-2C-BE-FB	data	confirmed	HUAWEI TECHNOLOGIES CO.,LTD
03/06/2021, 14:07:23	CC-2D-E0-A6-33-12	probe	unconfirmed	Routerboard.com
03/06/2021, 14:07:23	E0-D9-E3-73-07-6D	probe	unconfirmed	Eltex Enterprise Ltd.
03/06/2021, 14:07:23	38-B1-DB-25-65-63	probe/data	confirmed	Hon Hai Precision Ind. Co.,Ltd.
03/06/2021, 14:08:23	4C-49-E3-F9-FE-81	probe/data	confirmed	Xiaomi Communications Co Ltd
03/06/2021, 14:08:23	E0-DC-FF-F4-2B-C3	data	confirmed	Xiaomi Communications Co Ltd
03/06/2021, 14:08:23	C8-02-8F-95-A7-6A	data	confirmed	Nova Electronics (Shanghai) Co., Ltd.
03/06/2021, 14:08:23	0C-9D-92-6E-D9-20	probe/data	confirmed	ASUSTek COMPUTER INC.
03/06/2021, 14:08:23	D8-9E-61-36-DC-88	data	confirmed	Huawei Device Co., Ltd.
03/06/2021, 14:08:23	6C-C7-EC-F2-08-29	probe/data	confirmed	SAMSUNG ELECTRO-MECHANICS(THAILAND)
03/06/2021, 14:08:23	BB-27-EB-1B-45-D5	probe	unconfirmed	Raspberry Pi Foundation
03/06/2021, 14:08:23	40-23-43-32-8A-F9	probe	unconfirmed	CHONGQING FUGUI ELECTRONICS CO.,LTD.
03/06/2021, 14:08:23	10-D0-7A-E8-01-0C	probe	unconfirmed	AMPAK Technology, Inc.
03/06/2021, 14:08:23	24-FD-52-CC-B4-C6	probe	unconfirmed	Liteon Technology Corporation

Рис. 8. ***Страница с подробной статистикой: а – выпадающий список для выбора источника данных (точки доступа), б – вкладки с визуальным отображением статистики, в – таблица MAC-адресов***

нового способа анализа информационных потоков беспроводных сетей Wi-Fi, позволяющего проводить учет устройств в зоне покрытия сети и идентифицировать аномальную сетевую активность. В отличие от существующих решений метод позволит производить фильтрацию пешеходного, статического и автомобильного трафика, а также предоставит возможность идентифицировать подозрительную сетевую активность за счет идентификации фиктивных адресов и технологий виртуализации.

В ходе практических исследований разработанного метода была подтверждена его работоспособность, но с некоторыми ограничениями, преодоление которых запланировано в ходе планируемого совершенствования системы. В дальнейшем будет продолжена работа над правилами определения типа устройств, идентифицируемых внутри сети, поскольку данный функционал позволит отсеивать лишнюю информацию об устройствах, которые явно не идентифицируют пешехода, например, IoT-устройства. Из слабых сторон предложенного метода также можно выделить выбранный способ разделения потока на пешеходов, медленно проезжающих автомобилистов и иных субъектов, использующих разные средства передвижения. Данная функция также может быть доработана, что в перспективе повысит эффективность метода при анализе трафика не только внутри помещений, но и на оживленных улицах. ■

ЛИТЕРАТУРА

1. Булыгин М. В., Намиот Д. Е. Об использовании данных мобильных абонентов в цифровой урбанистике // Современные информационные технологии и ИТ-образование. – 2019. – № 3 (15). – С. 755–766.

2. Akhtar Z. U. A., Wang H. WiFi-based driver's activity recognition using multi-layer classification // Neurocomputing. V. 4, 2020. P. 12–25.

3. Suraweera N., Collings I.B., Hanly S.V., Winter A., Sorensen J., Li S., Johnson M., Ni W., Hedley M. Passive through-wall counting of people walking using WiFi beamforming reports // IEEE Systems Journal. V. 15 (4). 2020. P. 5476–5482.

4. Huang Z., Xu L., Lin Y. Multi-stage pedestrian positioning using filtered WiFi scanner data in an urban road environment // Sensors. V. 11 (20), 2020. P. 1–20.

5. Yao G., Kia D., Syed A., Jonathan C.; Muhammad A. and oth. Real-Time Human Activity Recognition System Exploiting Ubiquitous Wi-Fi Signals // In Proc. of the IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting (APS/URSI). Singapore, 04–10 December 2021. P. 1033–1034.

6. Zhengyang W., Sheng C., Wei Y., Yang X. Environment-Independent Wi-Fi Human Activity Recognition with Adversarial Network // In Proc. of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Toronto, ON, Canada, 06–11 June 2021. P. 3330–3334.

7. Exploiting Wi-Fi Signals for Human Activity Recognition // In Proc. of 12th International Conference on Information and Communication Systems (ICICS). Valencia, Spain, 24–26 May 2021. P. 245–250.

8. Marco B., Valentina B., Ilaria De M., Paolo C. An unobtrusive Wi-Fi system for human monitoring // In Proc. of the IEEE 7th International Conference on Consumer Electronics. Berlin, Germany, 03–06 September 2017. P. 219–223.

9. Basinya E. A., Merzadinova G. T., Zakirova A. B., Akhayeva Z. B. et. al. Decentralized approach for collecting and processing data of the enterprise information infrastructure // J. of Theoretical and Applied Information Technology. 2022. V. 100, № 3. P. 788–798.

10. Zakirova A. B., Basinya E. A., Kantureyeva M. A., Akhmetova A. Z., Akhaeva Z. V. Intelligent support in making technical decisions in the enterprise information infrastructure // J. of Theoretical and Applied Information Technology. 2021. V. 99, № 13. P. 3144–3154.

Информационная безопасность современного предприятия: парольная защита

En **Information Security of Advanced Company: Password Protection**

M. Yu. Ivanov,
PhD (Eng.), Associate Professor
nis@brstu.ru

M. V. Sygotina,
PhD (Eng.), Associate Professor
msygotina@bk.ru

M. Yu. Vakhrusheva,
PhD (Phys./Math.), Associate Professor
mvahr@yandex.ru

Bratsk State University

V. V. Nadrshin,
PhD (Eng.)
nadrshin@istu.edu

Irkutsk National Research Technical University

The article presents the results of research on the implementation of password protection. The types of passwords used in practice are considered, with illustrations, their advantages and disadvantages are analyzed with examples. Taking into account the current normative documents, recommendations are proposed for the formation of strong user passwords and the actions maintain the relevance and functionality of password protection. Using the high-level programming language C++, various options for the password verification process are considered in detail. In addition to the complete source codes of computer programs, detailed comments on the logic of their functioning are given.

Keywords: information security, data protection, access control, password, identification, authentication

В работе приведены результаты исследований по реализации парольной защиты как способа обеспечения информационной безопасности. Рассмотрены разновидности используемых на практике паролей, с иллюстрацией на примерах проанализированы их достоинства и недостатки. С учетом действующих нормативных документов предложены рекомендации по формированию надежных пользовательских паролей и действия специалистов по информационной безопасности по поддержанию актуальности и функционала парольной защиты. С помощью языка программирования высокого уровня C++ подробно рассмотрены различные варианты процесса проверки пароля. Помимо полных исходных кодов программ для ЭВМ даны подробные комментарии логики их функционирования.

Ключевые слова: информационная безопасность, защита данных, контроль доступа, пароль, идентификация, аутентификация, программное обеспечение

Михаил Юрьевич Иванов,
кандидат технических наук, доцент
nis@brstu.ru

Марина Владимировна Сыготина,
кандидат технических наук, доцент
msygotina@bk.ru

Марина Юрьевна Вахрушева,
кандидат физико-математических наук, доцент
mvahr@yandex.ru

Братский государственный университет

Владимир Вагизович Надршин,
кандидат технических наук
nadrshin@istu.edu

Иркутский национальный исследовательский технический университет

Введение

В настоящее время одним из наиболее распространенных методов защиты от несанкционированного доступа (НСД) к корпоративным данным являются идентификация и аутентификация (проверка подлинности) пользователя [1]. К этому типу средств обеспечения информационной безопасности (ИБ) можно отнести:

- парольную защиту;
- «привязку» программного обеспечения к ЭВМ пользователя;
- программно-аппаратные системы защиты (электронные ключи).

В первом случае «ключевую» информацию вводит сам пользователь, во втором – она содержится в уникальных параметрах компьютерной системы, а в третьем – «ключевые» данные считываются с микросхем электронного ключа.

Парольная защита является наиболее простым и дешевым способом обеспечения ИБ, поскольку ее реализация и дальнейшее использование не требует больших затрат времени, сил и ресурсов ЭВМ: ведь пароль, по сути, представляет собой определенную последовательность знаков и символов некоторого алфавита.

Большинство парольных средств защиты использует логические механизмы верификации, сводящиеся к сравнению введенного пароля с содержащимся в системе образцом

и предоставлении или непредоставлении доступа в зависимости от результатов проведенной проверки [2].

Парольная защита очень актуальна для средних и крупных предприятий, располагающих большими объемами информационных ресурсов, в том числе распределенных и с удаленным доступом, самым разнообразным электронно-вычислительным оборудованием и ПО [3–7].

Вопреки устоявшемуся мнению, большинство нарушений информационной безопасности (до 65 %) обусловлено небрежным отношением и непреднамеренными ошибками самих работников организации, тогда как доля внешних проникновений не столь значительна [8].

Теоретические основы организации парольной защиты

Использование парольной защиты, помимо собственно контроля доступа, дает пользователю и ощущение определенного комфорта. Пароли, как правило, рассматриваются в качестве ключей для входа в информационную систему, но они могут использоваться и для других целей: блокирования записи или копирования конфиденциальных данных, подтверждения проведения операции, запуска определенного ПО и т. д. То есть во всех случаях, требующих твердой уверенности в том, что соответствующие действия будут производиться только штатными пользователями из числа работников предприятия [9].

Используемые сегодня пароли можно классифицировать следующим образом.

Пароли, устанавливаемые пользователем

Несмотря на распространенность, пароли этой группы редко являются надежными. В большинстве случаев пользователи ЭВМ действуют примерно одинаково. Работнику необходимо время, чтобы начать мыслить нестандартно, поэтому в качестве пароля он задействует ту информацию, которой пользуется постоянно и которую он точно не забудет. Иначе говоря, пользовательские пароли зачастую создаются в спешке, а последующая их замена на более надежные варианты происходит не всегда.

Типовыми неудачными пользовательскими паролями считаются имена, даты рождения, номера телефонов и страховок, паспортные данные, находящиеся в постоянном обиходе очевидные слова и т. д. В последние годы активно разрабатываются меры, не позволяющие пользователю создать неудачный пароль. Например, информационная система может требовать, чтобы пароль включал в себя строчные и заглавные буквы вперемешку с цифрами, а заведомо очевидные пароли отвергаются. Существует немалое количество специальных инструментов, которые анализируют пароли и определяют уровень их надежности.

Таким образом, несмотря на заявленный выше самостоятельный статус, пользовательские пароли в чистом виде таковыми не являются.

Пароли, генерируемые системой

Такие пароли имеют нескольких разновидностей: системное ПО может использовать полностью случайную последовательность (точнее, псевдослучайную, поскольку всегда существует вероятность генерации такой же последовательности с помощью другого ПО) символов вплоть до выбора регистров, алфавитов, цифр, пунктуации, длины или же применять в генерирующих процедурах какие-либо ограничения. Так, информационная система может формировать пароли, извлекая символы для них из списка обычных или ничего не значащих слов, заранее заложенных в словарь.

Пароли, генерируемые системой, безусловно, надежны, но эта надежность имеет и обратный эффект. Работники предприятия, опасаясь забыть свои пароли, начинают записывать их на всевозможные материальные носители. Следовательно, самостоятельное создание пользователями паролей в некоторых ситуациях может выглядеть даже более предпочтительно. Разумеется, качество пароля должно быть в любом случае проверено и подтверждено системными администраторами предприятия.

Кроме того, излишне сложные и нигде не записанные пароли работники неизбежно будут забывать, и специалистам по ИБ придется тратить значительное количество времени на их восстановление.

Полуслова

Пароли данной группы частично создаются пользователем, а частично – информационной системой. Это значит, что если даже пользователь придумает легко угадываемый пароль, то специальное ПО дополнит его своими символами, образовав более сложный и надежный пароль типа «Газпром5R#g».

Ключевые фразы

Использование в качестве паролей ключевых фраз хорошо тем, что они, как правило, достаточно длинные, их трудно угадать, но зато легко запомнить. Они могут быть вполне осмысленными (например, «Очень сложный пароль») или не иметь смысла (например, «Бегущий по небу»).

К концепции ключевых фраз можно отнести и пароли, представляющие собой акронимы или бэкронимы, образованные из начальных букв ключевой фразы в прямом или в обратном порядке соответственно. Пароли в виде акронимов или бэкронимов достаточно надежны, а пользователь в качестве ключевой фразы может использовать легко запоминающееся предложение или строчку из текста хорошо знакомого романа, стихотворения, песни и т. п.

Интерактивные последовательности «вопрос – ответ»

Использование данного вида парольной защиты предполагает ответы пользователя на вопросы, как правило, личного плана: «Марка автомобиля», «Прозвище в детстве», «Любимое блюдо» и т. д. Несмотря на неплохую идею реализации, интерактивные последовательности не получили широкого распространения и сейчас почти не используются. Причина непопулярности защиты типа «вопрос-ответ» кроется в раздражающих прерываниях в работе для аутентификации пользователя. Вместе с тем, отказ от каких-либо средств защиты может иметь самые

негативные последствия. Поэтому руководству предприятия не стоит идти на поводу у своих работников, смягчая требования эксплуатации информационных систем и, тем самым, создавать потенциальную возможность нарушения ИБ.

Базовые требования к надежным паролям

Бесконтрольность в использовании паролей повышает риск НСД к информации, мошеннические и другие действия, которые могут нанести материальный вред и ущерб репутации предприятия [10–12].

С учетом изложенного ранее сформулируем базовые требования, предъявляемые к достаточно надежным паролям.

1. *Разнообразие используемых символов.* Наличие как прописных, так и строчных букв из разных алфавитов, цифр (одна и более), нецифровых и неалфавитных символов.

2. *Определенная длина.* Так, длина обычных пользовательских паролей работников предприятия должна составлять не менее 8 символов, паролей пользователей сетевого оборудования и ПО – не менее 10 символов, сервисных и разделяемых (общих) паролей – не менее 14 символов, паролей локальных и доменных администраторов – не менее 15 символов.

3. *Периодичность смены.* Пароли локальных и доменных администраторов рекомендуется менять каждые 60 дней, обычные пользовательские пароли – каждые 90 дней, сервисные и разделяемые пароли – не реже двух раз в год, пароли пользователей сетевого оборудования и ПО – не реже одного раза в год [13–14].

Кроме того, существуют и общие рекомендации, соблюдение которых поможет работникам предприятия избежать компрометации даже самого надежного пароля:

- не записывать пароль на бумагу и не хранить его в памяти телефона, не соглашаться на то, чтобы пароль был сохранен каким-либо ПО или интернет-браузером, хотя такую опцию последние предлагают постоянно, мотивируя это действие удобством для пользователя;
- не передавать пароли по информационно-телекоммуникационным сетям в незашифрованном виде [15];
- не сообщать свой личный пароль коллегам по какому бы то ни было поводу;
- не использовать в ходе работы встроенные в оборудование или программное обеспечения идентификаторы, назначив пароли, отличные от установленных производителем продукта;
- в случае увольнения или смены полномочий сотрудников немедленно заменять пароли, к которым они имели доступ.

Врезка 1

```
#include <iostream>
#include <string>

using namespace std;

int main()
{
 setlocale(0, «»);
 string correct_password = «TopSecret»;
 string employee_password;
 cout << «Введите пароль: «;
 getline(cin, employee_password);
 if (employee_password == correct_password)
 {
 cout << «Доступ разрешен» << endl;
 }
 else
 {
 cout << «В доступе отказано» << endl;
 }
 system(«pause»);
 return 0;
}
```

Практическая реализация парольной защиты

Программно-технические компоненты средств защиты данных являются весьма объемной составляющей ИБ. Особую важность имеет надежность реализации механизма проверки пользовательских паролей.

На врезке 1 приведен код программы для ЭВМ на языке программирования высокого уровня C++ для защиты от НСД к корпоративным ресурсам.

Данная программа для ЭВМ не содержит каких-либо ошибок, но ее недостатком можно считать отсутствие функций, крайне полезных для выполнения одних и тех же действий.

Осуществим процесс проверки пароля с помощью функции. Несложно догадаться, что в рассмотренной выше ситуации для возвращения вычисляемого значения используется стандартный оператор языка C++ *return*. Но такой подход не является эффективным, если программа для ЭВМ включает в себя несколько подпрограмм.

Используем для проверки пароля функцию типа *void*, которая не возвращает никакого значения (иногда такие функции также называют процедурами) (врезка 2).

А теперь используем функцию, возвращающую значение в ходе проверки пароля. В данном случае функция *verification_password* имеет тип string, следовательно, она будет возвращать только значение типа *string* (строку) (врезка 3).

Первой выполняется функция main, которая, как известно, должна присутствовать в каждой программе, написанной на языке программирования C++. Затем объявляется переменная *employee_password* (также типа *string*) и выводится приглашение пользователю «Введите пароль». Введенный пароль попадает в строку *employee_password*, а дальше начинает

работать собственная функция *verification_password*. В качестве аргумента этой функции передается введенный пользователем пароль (аргументы – это переменные или константы вызывающей функции, которые будет использовать вызываемая функция). Следует отметить, что переменные и константы, объявленные в разных функциях, независимы друг от друга и могут даже иметь одинаковые имена.

Далее осуществляется проверка введенного пользователем пароля. Если пароль верен, то переменной *mistake_report* присваивается значение «Доступ разрешен», если пароль неверен, то переменной *mistake_report* присваивается значение «В доступе отказано».

После проведенной проверки пароля возвращаем переменную *mistake_report*. На этом работа функции *verification_password* закончена. Теперь в функции main то значение, которое возвратила функция *verification_password*, присваивается новой переменной *mistake_rpt*, и это значение (строка) выводится на экран монитора.

Реализуем возможность повторного ввода пароля. Это действие оптимально выполнить с помощью рекурсии: операции, в ходе которой функция вызывает саму себя (врезка 4).

Возможность повторного ввода пароля не лишена целесообразности, поскольку позволяет, например, не перезагружать ЭВМ при ошибочно введенном пользователем пароле.

Заключение

В результате анализа различных подходов по формированию парольной защиты с учетом современных требований ИБ можно сделать следующие выводы.

Пароли, самостоятельно устанавливаемые пользователями, бывают качественными крайне редко. Сложность паролей, генерируемых различными информационными системами, на практике часто оказывается обесцененной самими работниками предприятия, записывающими и сохраняющими выданные им пароли. Эффективные интерактивные последовательности «вопрос – ответ» не

Врезка 2

```
#include <iostream>
#include <string>

using namespace std;

void control_password (string password)
{
 string correct_password = «TopSecret»;
 if (password == correct_password)
 {
 cout << «Доступ разрешен» << endl;
 }
 else
 {
 cout << «В доступе отказано» << endl;
 }
}
int main()
{
 setlocale(0, «»);
 string employee_password;
 cout << «Введите пароль: «;
 getline (cin, employee_password);
 control_password (employee_password);
 system(«pause»);
 return 0;
}
```

Врезка 3

```
#include <iostream>
#include <string>

using namespace std;

string verification_password (string password)
{
 string correct_password = «TopSecret»;
 string mistake_report;
 if (password == correct_password)
 {
 mistake_report = «Доступ разрешен»;
 }
 else
 {
 mistake_report = «В доступе отказано»;
 }
 return mistake_report;
}

int main()
{
 setlocale(0, «»);
 string employee_password;
 cout << «Введите пароль: «;
 getline (cin, employee_password);
 string mistake_rpt = verification_password (employee_password);
 cout << mistake_rpt << endl;
 system(«pause»);
 return 0;
}
```

Врезка 4

```
#include <iostream>
#include <string>

using namespace std;

bool password_is_correct (string password)
{
 string correct_password = «TopSecret»;
 if (correct_password == password)
 return true;
 else
 return false;
}

void get_password()
{
 setlocale(0, «»);
 string employee_password;
 cout << «Введите пароль: «;
 getline(cin, employee_password);
 if (!password_is_correct(employee_password))
 {
 cout << «В доступе отказано» << endl;
 get_password(); // рекурсия
 }
 else
 {
 cout << «Доступ разрешен» << endl;
 }
}

int main()
{
 get_password();
 system(«pause»);
 return 0;
}
```

получили признания из-за раздражающего пользователей алгоритма работы.

Таким образом, наиболее надежными средствами парольной защиты являются ключевые фразы и полуслова.

В практической части исследования реализованы различные механизмы проверки правильности введенного пароля, оказывающие непосредственное влияние на безопасность конфиденциальных данных. Предложенные методы верификации могут использоваться в виде надстройки штатных корпоративных средств защиты, а при использовании в качестве пароля информации личного плана – как дополнительный способ аутентификации, снижающий вероятность подмены пользователя. ■

ЛИТЕРАТУРА

1. Сабанов А. Г. Принципы классификации систем идентификации и аутентификации по признакам соответствия требованиям информационной безопасности // Электросвязь. – 2014. – № 2. – С. 6–9. EDN: RYMGAF.

2. Иванов М. Ю. Современные информационные технологии криптографической защиты данных // Системы. Методы. Технологии. – 2015. – № 3 (27). – С. 73–78. EDN: UKWGJR

3. Malsagov B. S., Ivanov M. Yu., Natalevich L. F. Structural features of accounting automation application // Journal of Physics: Conference Series. – 2021. – V. 2032, № 1. – Art. 012128. DOI: 10.1088/1742-6596/2032/1/012128.

4. Арыпбекова К. Б., Искендеров А. У. Информационные технологии в системе национальной безопасности // Вестник Кыргызского государственного университета им. И. Арабаева. – 2018. – № 1. – С. 110–113. EDN: YUDXDF.

5. Ивличев П. С., Ивличева Н. А. Информационные технологии обеспечения безопасности платежных средств в свете современных тенденций в киберпреступности // Экономика и предпринимательство. – 2017. – № 2–1 (79). – С. 135–139. EDN: YGAUWH.

6. Королев В. И., Гаврилов В. Е. Информационные системы цифровой экономики и подходы к обеспечению их ИБ // Системы высокой доступности. – 2019. – Т. 15, № 1. – С. 38–46. DOI: 10.18127/j20729472-201901-05.

7. Мирошниченко М. А., Бондаренко А. А., Пиналова Е. В. Актуальные проблемы обеспечения информационной безопасности систем электронного документооборота в рамках цифровой трансформации // Вестник Академии знаний. – 2020. – № 1 (36). – С. 137–142. DOI: 10.24411/2304-6139-2020-00024.

8. Alchinov A. I., Polovneva S. I., Ivashchenko G. A. Methods of testing computer systems for various kinds of penetration // Journal of Physics: Conference Series. – 2021. – V. 2032, № 1. – Art. 012134. DOI: 10.1088/1742-6596/2032/1/012134.

9. Зинатова А. А. Программное обеспечение по информационной безопасности – важный объект интеллектуальной собственности в эпоху цифровых технологий // Финансовые рынки и банки. – 2018. – № 2. – С. 15–18. EDN: MQYRIR.

10. Daudov Kh. A., Zinoviev A. A., Gavrilova Zh. L. Principles of protection, storage and movement of documents during electronic document flow within and outside the organization // IOP Conference Series: Materials Science and Engineering. – 2021. – V. 1111, № 1. – Art. 012022. DOI:10.1088/1757-899X/1111/1/012022.

11. Markova S., Druzhinina T. Ya., Zinoviev A. A. Modifying event log files in operating systems // Journal of Physics: Conference Series. – 2021. – V. 2032, № 1. – Art. 012139. DOI: 10.1088/1742-6596/2032/1/012139.

12. Svirbutovich O. A., Zhigalov K. Yu., Patrusova A. M. Static file analysis to detect rootkits in the system // Journal of Physics: Conference Series. – 2021. – V. 2032, № 1. – Art. 012137. DOI: 10.1088/1742-6596/2032/1/012137.

13. Вихляев С. А., Белов И. В., Кононова М. А. Применение программной системы «Digital Security Office» для проведения аудита безопасности информационной системы обработки персональных данных // Молодой ученый. – 2014. – № 8. – С. 75–78. EDN: SFRXPV.

14. Филяк П. Ю., Бартов М. О., Красномовец А. В. Обеспечение информационной безопасности при использовании систем электронного документооборота (ECM-систем) // Информация и безопасность. – 2015. – Т. 18, № 4. – С. 576–579. EDN: VADPYV.

15. Иванов М. Ю. IT-технологии в вопросах обеспечения информационной безопасности предприятий // Системы. Методы. Технологии. – 2014. – № 1 (21). – С. 78–82. EDN: RZKKJD.

Модели оценки киберустойчивости транзакций в СУБД

Выполнение требований нормативных документов к защищенности объектов критической информационной инфраструктуры ставит задачу по разработке средств нейтрализации компьютерных атак в условиях целенаправленных воздействий злоумышленников и выдвигает новые требованиями к защищенности и своевременности обработки данных в системах управления базами данных (СУБД). В статье предлагается подход обеспечения целостности базы данных автоматизированной системы управления проектированием кораблей (БД АСУ ПК) на основе самоконтроля семантики функционирования СУБД, вследствие чего происходит подавление запуска любых опасных процессов в памяти ЭВМ, так как это будет запрещено оператором компьютерной системы. В то же время, фиксация попыток запуска посторонних процессов будет фиксироваться, так как это может быть признаком наличия недекларируемых возможностей программного обеспечения или хакерских действий.

Ключевые слова: системы управления базами данных, безопасное функционирование, телерадиовещание, подавление опасной функциональности, научно-методический аппарат

Диана Евгеньевна Воробьева,
ведущий программист отдела эксплуатации АСУ ПК

dinvor@mail.ru

АО «Невское проектно-конструкторское бюро»

Евгений Германович Воробьев,
доктор технических наук, доцент, заведующий кафедрой «Информационная безопасность»

vrbyug@mail.ru

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Введение

В настоящее время существует 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 при проектировании кораблей на основании как ведомственных, так и общероссийских требований. Для разрешения данного противоречия может быть предложен следующий подход: обеспечение целостности БД АСУ ПК в условиях роста угроз безопасности на основе самоконтроля семантики функционирования СУБД.

Полезность предлагаемого в статье научно-математического аппарата (моделей) по отношению к потребностям практики, заключается в доведении их до прототипа программной системы обеспечения целостности БД (СУБД) АСУ проектирования кораблей, который может быть использован в составе конкретных АСУ ПК и СУБД в их составе.

Этот прототип актуализирован применительно к работе в старейшем в Российской Федерации проектно-конструкторском бюро надводного кораблестроения – АО «Не-

En Models for Assessing the Cyber Resilience of Transactions in a DBMS

D. E. Vorobyova,
Lead Programmer of ACS Operation Department

dinvor@mail.ru

JSC «Nevsky Design Bureau»

E. G. Vorobyov,
PhD (Eng., Grand Doctor) Associate Professor, Head of Information Security Department

vrbyug@mail.ru

Saint-Petersburg State Electrotechnical University «LETI»

Compliance with the requirements for the security of critical information infrastructure facilities sets the task of developing means of neutralizing attacks in conditions of targeted impacts and puts forward new requirements for the security and timeliness of data processing in the DB. This article proposes an approach to ensure the integrity of the ICS database based on self-control of the semantics of the DB functioning. The result will be the suppression of the launch of any dangerous processes in the computer memory, since the operator of the computer system will not allow this. At the same time, the fixation of attempts to launch extraneous processes will be recorded, as this may be a sign of the presence of undeclared software capabilities or hacker actions.

Keywords: database management systems, safe functioning, television and radio broadcasting, suppression of dangerous functionality, scientific and methodological apparatus

вское ПКБ». Использование прототипа позволяет на практике повысить защищенность обработки данных в СУБД. В частности, в рассмотренных в исследовании условиях моделирования обеспечивается увеличение своевременности выявления заранее неизвестных сигнатур атак и реагирования на последние.

Структурно-функциональная модель СУБД

Необходимая по условиям поставленной задачи корректность принятия решения о состоянии СУБД обеспечивается на основе использования информации об объекте подключения к данным: идентифицируемом объекте, имеющем подключение к сети взаимодействия и способным посылать или получать сообщения [1].

В общем случае каждый объект обрабатывает следующие типы информации:

- информацию об устройстве;
- генерируемые управляющие воздействия на другие объекты;
- получаемые управляющие воздействия на другие объекты (запросы к данным);
- сообщения об ошибках [2].

Объективно присутствует недостаточность применяемого в существующих методах анализа парных отношений для выявления инцидентов безопасности. Действующий подход состоит в том, что событие безопасности АСУ заключается в изменении количества вершин графа, количества ребер графа или параметров вершин и ребер графа.

В действительности, при неизвестной заранее опасной функциональности объектов анализа затруднена сама возможность анализа, не говоря уже об отсутствии необходимой исходной информации.

Набор взаимодействующих компонентов АСУ ПК, в том числе с БД, представляется в виде графа G, где каждое устройство характеризуется набором параметров [3, 6].

Состояние защищенности БД γ характеризуется моментом времени t, состоянием транзакций v_i, предикатами операций p_i, и другими параметрами, позволяющими создать структурно-функциональную модель СУБД.

$\gamma: T \rightarrow V;\ V = \{v_1, v_2, \ldots, v_n\},$

$T = \{t_1, t_2, \ldots, t_n\},$

$P_i = \{\varphi(t_i), p_{i_1}, p_{i_2}, \ldots, p_{i_j}\},\ P_i \in P;$

$\varphi(t_i)$ – значимый период функционирования;

$p_{i_1}, p_{i_2}, \ldots, p_{i_j}$ – значимые параметры;

$E = \{e_1, e_2, \ldots, e_m\}$ – набор ребер/связей;

дискретный поток сообщений $M = \{M_1, M_2, \ldots, M_n\}$, представляющий собой последовательность парных отношений;

неявные взаимосвязи $\{t_i, t_j\}$;

дискретный поток событий $E_v = \{ev_1, ev_2, \ldots, ev_n\}$

$\xi: M \rightarrow Ev.$

При этом как при анализе уязвимостей, так и при эвристическом анализе возникает необходимость анализа сложного графа (см. рисунок).

Математическая модель оценки уровня безопасности транзакций в СУБД

Пусть объект оценки – база данных АСУ (БД), обладающая целевой функцией (ЦФ).

ЦФ БД представляет собой множество вычислительных процессов, каждому из которых соответствует набор функций F_i, выполняемых компонентами информационной составляющей АСУ ПК:

$F = \{F_1, F_2, \ldots, F_n\},$

$\forall F_1 = \{f_1^i, f_2^i, \ldots, f_k^i\}$

с заданным отношением порядка. Каждый процесс характеризуется:

- обменом данными между компонентами информационной составляющей распределенной БД;
- диапазоном допустимых значений параметров запросов и действий СУБД, гарантирующих корректное протекание процесса [4, 5].

Требуется:

1) *построить модель функционирования БД и показать ее полноту:*

- модель должна описывать ЦФ и отношения между функциями $f_k, \ldots, f_m \in F_i$;
- модель должна описывать последствия различных типов компьютерных атак Z;
- каждая компьютерная атака Z_i влияет на ЦФ:

$\forall_i f(Z_i, G): F \rightarrow F',\ F' \neq F$

и реализуется за время $\text{time}(Z_i)$;

2) *найти оператора раннего обнаружения атак на СУБД*: оператор обнаружения *Detect* доложен быть инвариантен к типу атак:

$\forall_i \exists Detect: (Z_i, G): \bar{f} = (\bar{f_n^i}, \bar{f_n^j}, \ldots)$

и обнаруживать аномалии в ЦФ за время, меньшее времени распространения атаки:

$(time(Direct(Z_i, G)) < time(Z_i);$

3) *найти оператор саморегуляции:* оператор саморегуляции *Reg* переводит СУБД в новое состояние, сохраняя ЦФ: $Reg(G): G \rightarrow G'', F'' = F$ и реконфигурирует СУБД за время, меньшее времени распространения атаки (с учетом обнаружения):

$time(Derect(Z_i, G)) + time(Reg(Z_i, G)) < time(Z_i);$

4) *найти оператор, позволяющий оценить киберустойчивость АСУ ПК и ее СУБД*: оператор оценки киберустойчивости *CybR* должен обеспечивать получение численного значения киберустойчивости, характеризующего качество выполнения саморегуляции СУБД, а оценка киберустойчивости должна быть найдена с использованием информации о ЦФ СУБД.

Предлагаемая модель позволяет обосновать пути повышения скорости реагирования на заранее неизвестную компьютерную атаку и ее нейтрализации, которые в дальнейшем использовались при разработке методики блокирования этих атак. Модель обладает следующими основными признаками научной новизны:

- в состав модели введены операции и параметры, формализующие реагирование на атаки с неизвестной сигнатурой;
- в состав модели введены формальные операции и критерий саморегуляции.

Система безопасности АСУ ПК для выполнения требований Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» должна

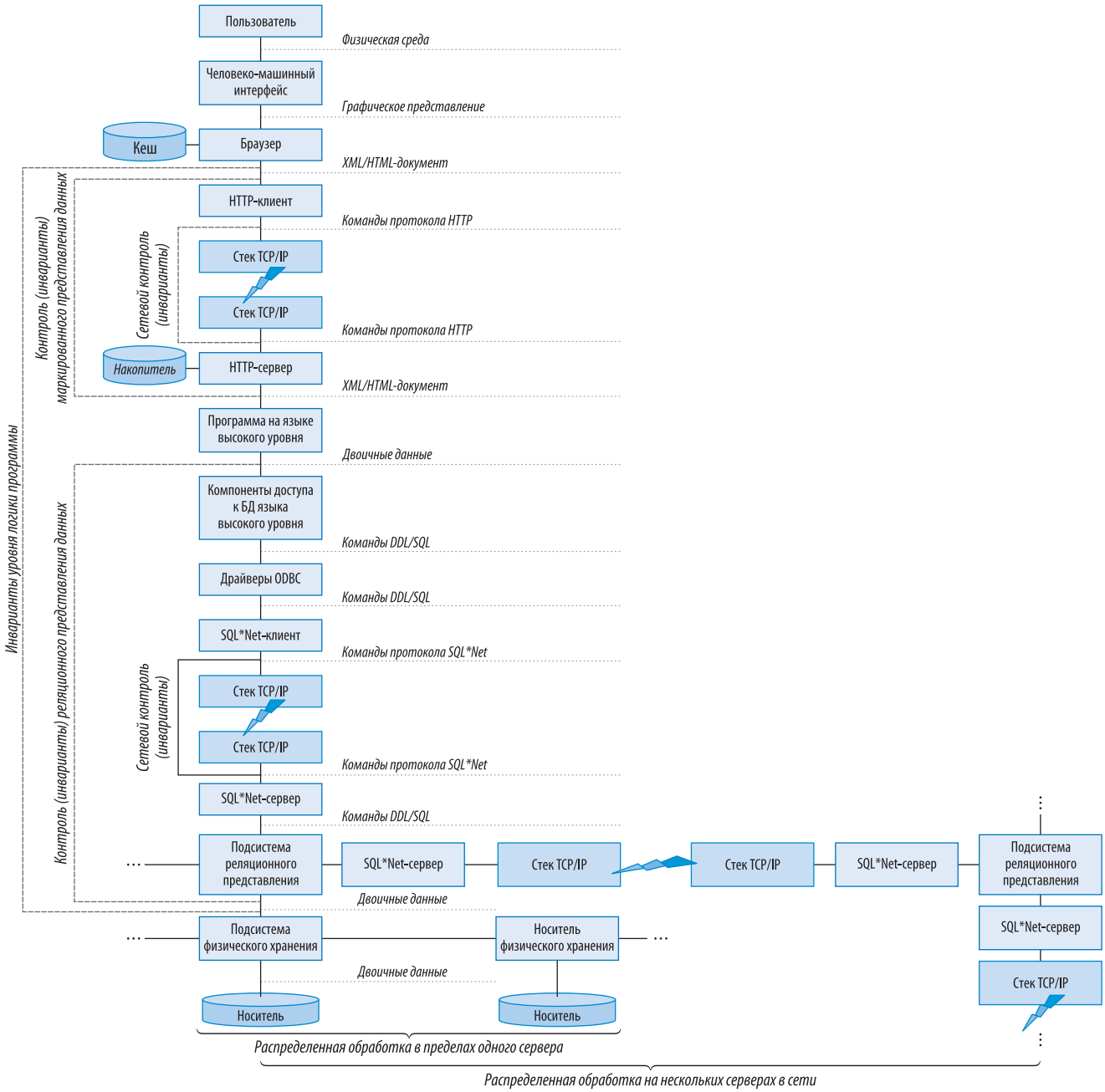


Рис. 1. ***Аналитический граф процесса функционирования СУБД***

обеспечивать автоматическое информирование о происходящих инцидентах государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации (ГосСОПКА). При расследовании инцидента в ГосСОПКА выполняется следующий процесс:

- назначение весовых коэффициентов каждому типу параметров событий в зависимости от типа обнаруживаемого инцидента;
- задание уровня, который будет означать, что если функция схожести принимает значения, превышающие данный уровень, то события с достаточной степенью силы взаимосвязаны между собой;
- вычисление корреляции между событиями путем использования значения функции схожести;
- сравнение полученного значения с пороговым уровнем;
- группирование взаимосвязанных событий.

Путем введения специальных программ-коконов система защиты обретает дополнительные шаги:

- получение меры схожести между двумя типами атрибутов:
  - корреляция символьных параметров;
  - корреляция числовых параметров.

Функции схожести символьных и числовых параметров проверяются программным путем ((1) и (2) соответственно) (см. врезку).

Применяемый в настоящее время в системах обнаружения вторжений подход (анализ устойчивости (самоподобия) системы фрактальными методами) состоит из следующих шагов:

- анализ периодичности многомерных временных рядов с исполь-

НОВОСТИ

Премия «Знание – 2022»

Главный редактор журнала «Защита информации. Инсайд», профессор Университета Иннополис С. А. Петренко включен в шорт-лист номинантов просветительской премии «Знание – 2022».

С. А. Петренко соревнуется за звание лауреата в номинации «За вклад в просвещение в сфере «Новые горизонты»». Он более 35 лет занимается преподавательской и научной деятельностью, является автором серии книг по кибербезопасности цифровой экономики РФ, регулярно проводит научные исследования по вопросам независимости технологического сектора России от импортных решений и является вдохновителем создания ряда отечественных кибертехнологий.

В ноябре номинанты, вошедшие в шорт-лист, провели очную защиту своих инициатив перед членами Почетного жюри, куда приглашены государственные деятели высшего звена, лидеры бизнеса и общественных организаций, известные деятели науки, культуры и искусства. В ходе своего выступления С. А. Петренко рассказал жюри о наиболее значимых проектах, в которых он принял самое активное участие:

- создании нового научного направления в области искусственного интеллекта – «Кибериммунология»;
- организации глобальной цифровой образовательной сети, с помощью которой на базе Университета Иннополис 20 тыс. преподавателей российских вузов прошли обучение в рамках подготовки кадров для цифровой экономики РФ;
- разработке вместе с зарубежными коллегами из ведущих университетов мира первого учебного руководства ООН по кибербезопасности.

Торжественная церемония вручения Премии «Знание» 22 лауреатам, выявленным в ходе работы жюри и онлайн-голосования, состоится 13 декабря в Государственном кремлевском дворце в Москве.

По материалам пресс-службы Российского общества «Знание»

Врезка

$$Sim_{cha}(event_i, event_j) = \sum_{k=1}^{p} \frac{\varphi(value_{ik}, value_{jk})}{p}; \quad (1)$$

$$Sim_{num}(event_i, event_j) = \frac{\sum_{f=1}^{n} \omega_f Sim_f(event_i, event_j)}{\sum_{f=1}^{n} \omega_f}. \quad (2)$$

При этом все проверки должны происходить в трансляторе таких программ:

$$Sim(event_i, event_j) = \mu Sim_{cha}(event_i, event_j) + (1 - \mu) Sim_{num}(event_i, event_j)$$

зованием автокорреляционной функции;
- вычисление фактора самоподобия (фактора Фано).

Предлагаемый подход предлагает сокращение размерности пространства методом главных компонент (МГК):
- построение ковариационной матрицы;
- поиск главных компонент;
- анализ влияния изменений показателей на значение главной компоненты.

Таким образом, реализация задачи состоит в уменьшении размерности временных рядов и ковариационной матрицы при анализе влияния изменений показателей транзакций и функционирования СУБД в составе АСУ ПК на основе вычисления фактора самоподобия.

Для обеспечения необходимой защищенности может быть разработан программный комплекс для «иммунизации» активных элементов СУБД (исполнимых файлов, файлов сценариев, SQL-запросов). Предлагаемым решением является принудительное ограничение функциональности активных элементов на основе списка реально декларируемых возможностей. На основе данного подхода авторами статьи был разработан и внедрен метод блокирования опасной функциональности ПО, реализующего транзакции в СУБД КАСУ в АО «Невское ПКБ». Методикой критериальной оценки в данном случае являлась методика оценки уровня безопасности транзакций в СУБД.

Заключение

Представленная в статье структурно-функциональная модель СУБД рассматривается впервые благодаря тому, что в состав модели введены операции и параметры, формализующие своевременность распознавания и подавления заранее неизвестных атак на БД АСУ ПК, на основе отказа от сигнатурного анализа приходящих команд управления и SQL-запросов. В состав модели введены формальные операции и критерий селекции таких команд за счет применения блокирующего транслятора и запрета на выполнение произвольных операций операционной системой.

Применение блокирующего транслятора, позволит, с одной стороны, отказаться в реальных системах от сигнатурного анализа команд управления СУБД, а с другой стороны, – увеличить защищенность таковых благодаря возможности блокирования запуска опасных процессов в памяти ЭВМ как при внешнем, так и при внутреннем их вызове. ■

ЛИТЕРАТУРА

1. Смирнова Н. А. Формирование оценочной модели устойчивости с использованием дискриминантного анализа. – Нижний Новгород: Вестник нижегородского ун-та им. Н. И. Лобачевского. – 2013. – № 3. – С. 235–238.

2. Безопасность объектов критической информационной инфраструктуры. Общие рекомендации. – М.: АРСИБ. – 2019. – 52 с.

3. Основы современных компьютерных технологий: учебник; [под ред. А. Д. Хомоненко]. – СПб: Изд-во БХВ. – 2005. – 672 с.

4. Горбань И. И. Феномен статистической устойчивости. – М.: Наука. – 2014. – 444 с.

5. Тутубалин В. Н. Теория вероятностей. – М.: Изд-во Московского ун-та. – 1972. – 230 с.

6. Горбань И. И. Теория гиперслучайных явлений: физические и математические основы. – М: Наука. – 2011. – 318 с.

Оценка технических характеристик РЛСАР с использованием акустически возбужденных пассивных резонаторов

Рассмотрены результаты исследования в США и Великобритании советского закладочного устройства. Приведено разъяснение принципов работы системы акустической разведки (РЛСАР). Показано влияние параметров объемного резонатора и частоты зондирующего сигнала на результаты применения устройства.

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»

Анализ советской пассивной закладки в США и Великобритании

В статье [1] было рассказано об обстоятельствах обнаружения американцами советской пассивной закладки в Москве. Далее события развивались следующим образом. 16–17 сентября 1952 года в ФБР прошли первичные исследования находки, так как изначально было непонятно, как закладочное устройство (ЗУ) работало: у него не было никаких активных компонентов. Прозвали найденный предмет «The Thing» (вещь, штука, предмет, а также новейшая, самая последняя или самая актуальная тенденция, мода или стиль), в отечественной историографии закладка, по названию операции по ее внедрению, получила называние «Златоуст». ФБР отправило устройство в свою Техническую лабораторию, где ее осматривали сотрудники радио- и электрической секций.

Выводы были сделаны интересные. Во-первых, что The Thing не содержит металлических деталей (?), поэтому не обнаруживалась ранее с помощью металлодетектора. Во-вторых, в «гербе» обнаружены две полости, из которых одна (малая) содержала ЗУ, вторая же (большая) была пустой (рис. 1). Позже в ФБР установили, что габаритные размеры второй полости соответствуют уже известному американцам советскому радиомикрофону с батарейками [2–4].

Первый вывод – явно фантастический для середины XX века: приемо-передающая антенна (проводник) не обнаруживается металлодетектором! Думается, что в данном случае

En Evaluation of Technical Characteristics ARRS Using Acoustically Generated Passive Resonators

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

The results of the study of the Soviet stowage device in the USA and Great Britain are considered. An explanation of the principles of operation of the acoustic reconnaissance system (RLSAR) is given. The influence of the parameters of the cavity resonator and the frequency of the probing signal on the results of the application is shown.

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

Рис. 1. ***Две полости «герба»***

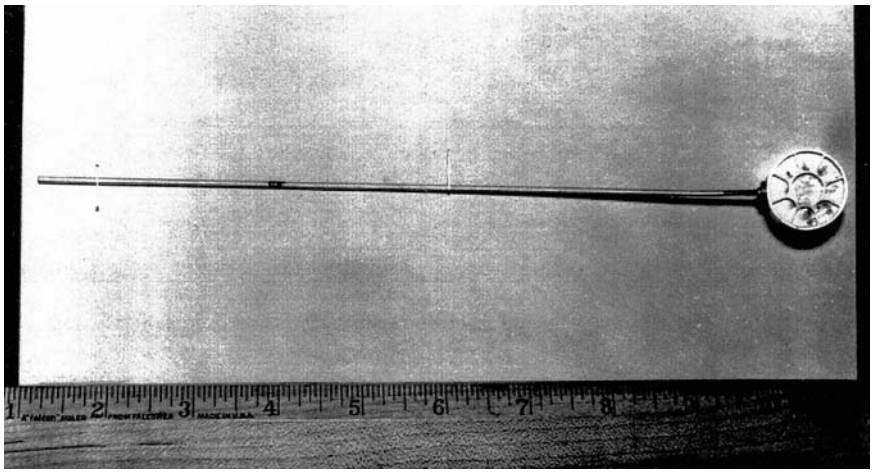


Рис. 2. ***Фотография «Златоуста» с длинной антенной с линейкой в дюймах из совершенно секретного отчета Госдепа США (декабрь 1952 года) [2]***

бюрократия победила физику. Между спецслужбами были хорошие отношения, а вывод о неметаллическом составе ЗУ позволял оправдать сотрудников Госдепа США в элементарной халатности: в ходе проведения входного контроля сувенира и последующих многочисленных проверок никто не удосужился провести по «гербу» металлоискателем и обнаружить длинную металлическую антенну (рис. 2).

Существует мнение, разрушающее все имеющиеся легенды о внедрении: изначально «герб» подарили пустым, а после входного контроля установили шедевр Л. С. Термена уже без участия пионеров. Причем резонатор решили использовать в последний момент, когда камуфляж под радиомикрофон был уже готов.

Однако не будем комментировать предварительные выводы, отметим только, что в технической лаборатории ФБР в 1952 году не нашлось ни генераторов, ни приемников с частотой свыше 400 МГц [5]! Пришлось позаимствовать необходимую аппаратуру у Национального бюро стандартов.

22 сентября 1952 года Президент США Гарри Трумен приказал создать Специальный комитет (*Special Committee*, SC) для анализа проблем безопасности в связи с обнаруженным The Thing из представителей Межведомственного комитета по вопросам внутренней безопасности и ЦРУ. Возглавил его специальный агент ФБР Эдвард С. Сандерс. Обратим внимание на следующее: в диппредставительствах США по всему миру выявлялись десятки ЗУ. Работы по анализу разведаппаратуры шли внутри ведомств, проходил рутинный процесс обмена информацией между силовыми структурами. А тут спустя всего неделю после обнаружения The Thing вопрос берет на контроль высшее военно-политическое руководство США. Это, конечно, прецедент!

На первом заседании SC, состоявшемся 1 октября 1952 года, на котором присутствовали представители армии, авиации и флота, были кратко изложены предварительные результаты расследования ФБР. 23 сентября 1952 года они были установленным порядком оформлены. Наиболее важными техническими выводами расследования ФБР были:

Устройство представляет собой объемный резонатор со встроенным конденсаторным микрофоном;

- длина антенны – $1^1/_2\lambda$ (интересно, что в ЦРУ длину антенны определили как $\lambda/2$. – *Примеч. авт.*);
- частота – между 1650 и 1800 МГц;
- хорошее качество перехватываемой речи;
- очень хорошая акустическая чувствительность [3].

6 октября 1952 года Президент США заслушал Директора ФБР о ходе расследования и поручил проводить работы совместно с военно-морской научно-исследовательской лабораторией (*Naval Research Laboratory*, NRL), обладающей существенными техническими и кадровыми возможностями. 13 октября 1952 года ФБР обратился к Отделу внутренней разведки с просьбой изготовления аналогов советского ЗУ. Для данной работы были привлечены инженерные лаборатории корпуса радиосвязи Армии США (*The Signal Corps Engineering Laboratories*, SCEL). Интересно отметить, что сотрудники SCEL знали, что в Bell Telephone Laboratories было разработано устройство для модуляции несущей частоты путем изменения физического размера резонатора.

На основании чертежей советского резонаторного микрофона, кото-

рые были предоставлены ФБР, SCEL сумел создать в менее чем месячный срок две его рабочие копии. Аппарат работал на частоте 1100 МГц и обладал отличной звуковой чувствительностью, потому что мембрана размещалась всего лишь в 25 мкм от диска (в оригинальной конструкции это расстояние составляло около 250 мкм). Устройство было испытано через фанерную стену с передатчиком низкой мощности, и был зафиксирован сигнал с АМ-модуляцией. Глубина модуляции составила 50 % – прекрасный результат! Предполагается, что ЦРУ также произвело свои собственные прототипы, основанные на чертежах, предоставленных ФБР.

По решению правительства Великобритании 28 октября 1952 года его представитель побывал в ФБР по поводу обнаруженного ЗУ. 3 ноября 1952 года ФБР провело 45-минутный брифинг по техническим вопросам с сотрудниками Управления специальных расследований (*Office of Special Investigations*, OSI). Данные подразделения сформированы в составе ВВС, Минюста и иных ведомств и по федеральному закону обеспечивают проведение независимых уголовных расследований, контрразведывательных и охранных операций. На совещании были озвучены следующие тезисы:

- рабочая частота устройства – 1700 МГц;
- устройство имеет серийный номер 11 (? – *Примеч. авт.*);
- устройство было испытано на расстоянии 75 футов (23 метра);
- до сих пор было найдено только одно подобное устройство;
- разрабатываются контрмеры [3].

Совместный подробный технический отчет ФБР и NRL об исследовании советского ЗУ был готов 1 декабря 1952 года и включал следующие документы:

- отчет об анализе и экспериментах лаборатории ФБР;
- детальные чертежи различного масштаба и фотографии;
- отчет NRL с информацией относительно проектирования средств противодействия.

12 февраля 1953 года Администрация Президента США запросило ФБР о возможности обследования территории Белого дома на предмет обнаружения полостных микрофонов [3].

Таким образом, можно выделить следующие знаковые даты:

- 4 августа 1945 года (по американской версии) в резиденции посла (по американской версии) произошло первое в истории внедрение ЗУ из состава РЛСАР;
- 10 сентября 1952 года имело место обнаружение РЛСАР в Спасо-Хаусе, резиденции посла США в Москве;
- 12 февраля 1953 года начались работы по защите помещений от РЛСАР (по крайней мере, в США).

К слову, существует не много технических средств разведки, имеющих точные даты для «празднования» юбилеев.

Высказывалось предположение, что американские чиновники понятия не имели, как работает устройство, и что они обратились за помощью к Великобритании. Например, на этом настаивал бывший сотрудник британской спецслужбы МИ-5 Питер Райт [7]. Представляется, что различные американские агентства тщательно исследовали прибор и имели хорошее представление о его работе. Можно предположить, что мнение Великобритании запросили, во-первых, чтобы проинформировать о находке, во-вторых, чтобы выслушать еще одно компетентное суждение. Следует заметить, что в связи с постепенным сворачиванием Британской империи и падением былой мощи своих спецслужб англичане любили распускать слухи о своем интеллектуальном и техническом превосходстве. Тем не менее, приведем и британскую версию событий.

По воспоминаниям самого Питера Райта, ему передали некое устройство, завернутое в хлопчатобумажную салфетку и упакованное в деревянный ящик, в котором, похоже, ранее хранились шахматные фигуры. Оно было цилиндрической формы и вместе с антенной имело 20 см в длину. Внутри цилиндра находился небольшой металлический винт в виде «гриба» с плоской вершиной для настройки всего изделия (по-видимому, за счет изменения электрической емкости). Позади

Питер Райт

«гриба» размещалась порванная тонкая диафрагма, игравшая роль мембраны микрофона.

Путем проб и ошибок Райту удалось отремонтировать поврежденную диафрагму, начать поиск резонансной частоты и, наконец, «заставить» The Thing заработать на частоте 800 МГц. Через два месяца состоялась торжественная демонстрация включения The Thing, во время которой, как писал Райт, «американские поисковики с ужасом смотрели на простоту всего этого устройства» [8].

Как видим, у ФБР, ЦРУ и МИ-5 сложились различные мнения даже об основной частоте зондирования.

Техническое описание The Thing

В распоряжении общественности есть несколько сделанных от руки чертежей The Thing, выполненных сотрудниками ФБР (рис. 3) и МИ-5 (рис. 4) в 1952 году [2, 13].

Обсудим возможную частоту работы устройства. Итак, в первоначальном расследовании ФБР утверждается, что длина антенны – $1\frac{1}{2}\lambda$, в то время как более поздний отчет ЦРУ определяет его как $\frac{1}{2}\lambda$. Некоторые специалисты утверждают, что длина волны должна быть $1\frac{1}{4}\lambda$ для частоты возбуждения и $\frac{3}{4}\lambda$ для частоты выхода. Существует предположение, что это полная длина волны (1λ). На рис. 5 приведены геометрические размеры антенны и вероятные длины волн [3].

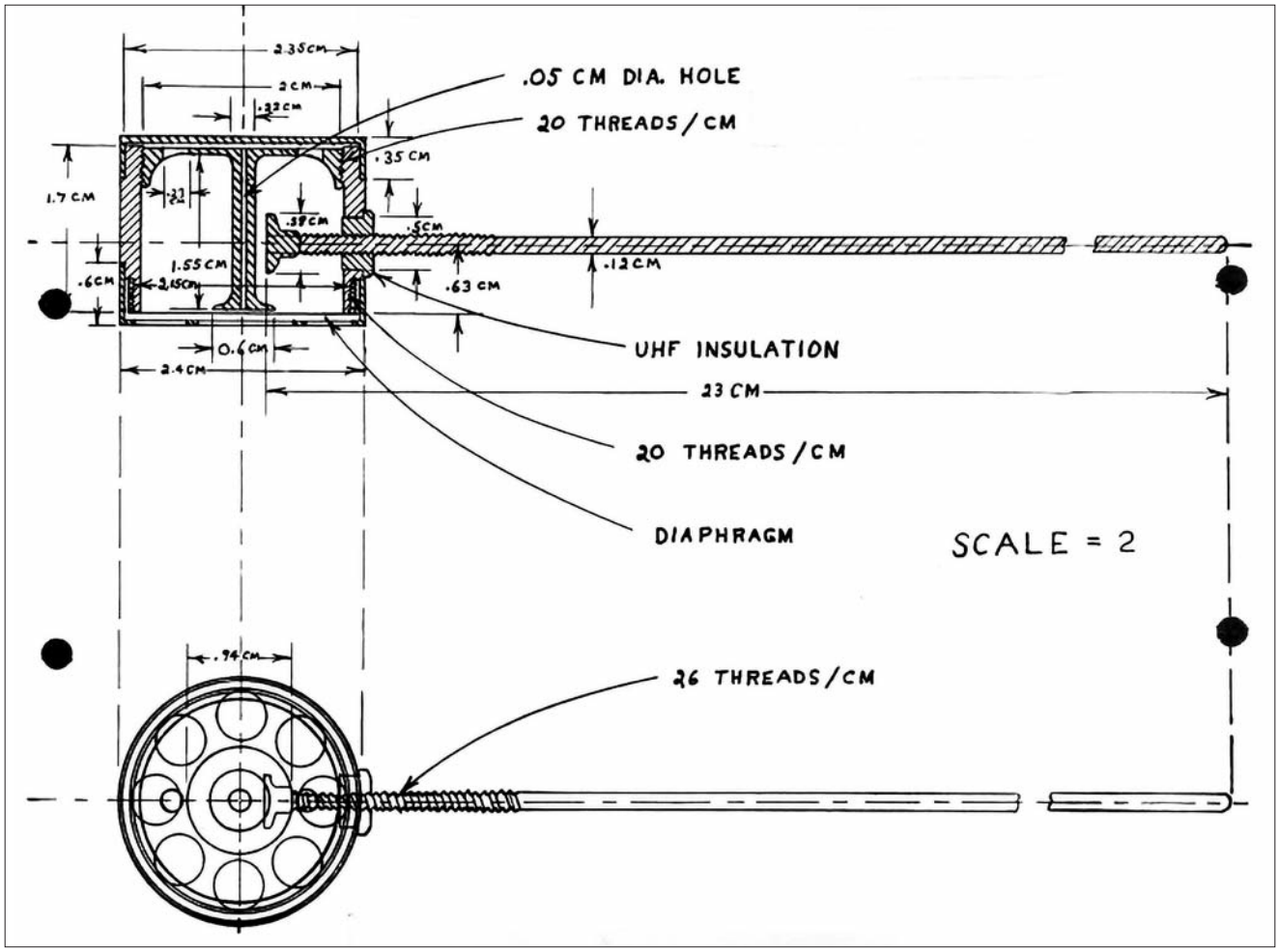


Рис. 3. ***Чертеж сотрудника ФБР***

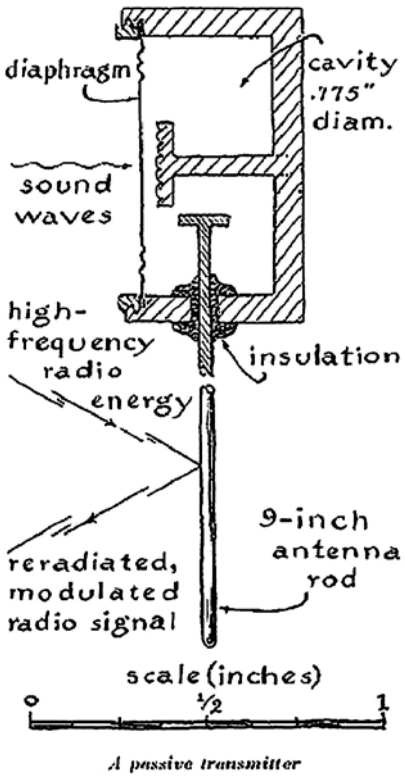


Рис. 4. ***Чертеж сотрудника МИ-5***

Приведенные на рис. 5 резонансные частоты антенны основаны на предположении, что антенна является идеальной и имеет длину 9 дюймов или ≈23 см. На практике же коррекция должна быть применена для компенсации так называемого краевого эффекта (емкостный краевой эффект увеличивает электрическую длину антенны, соответственно, длина антенны должна быть уменьшена). Если предположить, что указанный масштабный коэффициент примерно равен 0,9, это дает значение частоты между 1700 и 1800 МГц при длине антенны $1^1/_2\lambda$, что соответствует выводам лаборатории ФБР. Особенности построения резонатора, видимо, требуют подстройки приемника перед сеансом работы.

В работе [11] осуществлен следующий расчет частоты The Thing. Учитывая краевой эффект для антенны с отношением длины к диаметру 50:1, масштабный коэффициент должен быть $K_м = 0{,}955$. Расчет можно произвести по известной формуле

$$f_{рез} = c(N - 0{,}045)/4L_a, \qquad (1)$$

где c – скорость света, N – порядковый номер четверти волны, L_a – длина антенны, м. Соответственно, для антенны с длиной L_a= 0,228 м получаем следующие резонансные частоты: 314 МГц, 524 МГц, 972 МГц, 1301 МГц, 1630 МГц и 1959 МГц.

Понятно, что расчеты основываются на длине антенны 9 дюймов, которую «любезно» сообщил нам Питер Райт. Однако в России не принято измерять что-либо в дюй-

Рис. 5. ***Геометрические размеры антенны и вероятные длины волн***

мах, поэтому крайне маловероятным представляется такое «круглое» значение длины. Можно сделать вывод, что и остальные размеры не совсем точны. При L_a = 0,23 м (см. совершенно секретный чертеж ФБР [13]) первый резонанс будет на частоте 311 МГц. Можно также достаточно убедительно доказать, что резонанс был на частоте 330 МГц [2].

На рис. 6 показан макет The Thing, смоделированный на основе различных докладов и публикаций. Устройство состоит из медного цилиндра с полированной посеребренной внутренней поверхностью, который действует как высокочастотный объемный резонатор (эндовибратор). В центре находится диск регулируемой грибовидной формы с плоской поверхностью, выполняющий роль конденсатора в комбинации с очень тонкой мембраной, которая закрывает открытый конец резонатора. Антенна входит в полость через изолированное отверстие в боковой части цилиндра (емкостное соединение).

Мембрана или диафрагма в передней части корпуса цилиндра имела толщину всего 75 мкм. Настройка «ножки гриба» используется для увеличения или уменьшения емкости «гриба». Внешняя сторона «гриба» подвергнута механической обработке (имеет пазы) для уменьшения пневматического демпфирования диафрагмы. Согласно одному из источников, как уже упоминалось ранее, расстояние между «грибом» и диафрагмой изначально было 250 мкм, согласно другому – 230 мкм.

Размеры полости тщательно подбирались так, чтобы она была резонансной на заданной частоте. Затем ЗУ облучается сильным сигналом снаружи, как показано на рис. 7. Во избежание наложения излучающих и принимаемых волн вся геометрическая фигура должна была иметь форму равнобедренного треугольника [2, 14].

Любой звук в помещении (речь) заставляет мембрану вибрировать, что уменьшает/увеличивает пространство внутри полости, а также емкость между мембраной и «грибом». В результате ЗУ производит комбинацию амплитудной (АМ) и частотной модуляции. На практике советскими специалистами была использована только первая [3]. Из документов ЦРУ (рассекречены 25 апреля 2013 года) известно, что масса изделия составляла 31 г, а индуктивность – 0,01 мкГн [12].

Уникальность «Златоуста» была в том, что он не требовал электропитания и действовал так же, как зеркало при отражении света [14]. Отметим, что в первоначальных отчетах о расследовании предполагается, что частота зондирования была такой же, как и резонансная частота. Хотя это создает технические ограничения, такие как перегрузка приемника отраженными от фона сигналами, именно такой сценарий признан наиболее вероятным.

Теоретически можно было также использовать гармоники сигнала зондирования для уменьшения влияния передатчика на приемный тракт. Однако для того чтобы резонатор генерировал 2-ю и 3-ю гармоники зондирующей частоты, он должен обладать нелинейными свойствами (например, иметь тонкий окисленный слой между контактами, подобно полупроводнику – диоду). Этот эффект не является устойчивым, и его поведение было бы трудно предсказать и воспроизвести. Поэтому признано маловероятным, что советский ре-

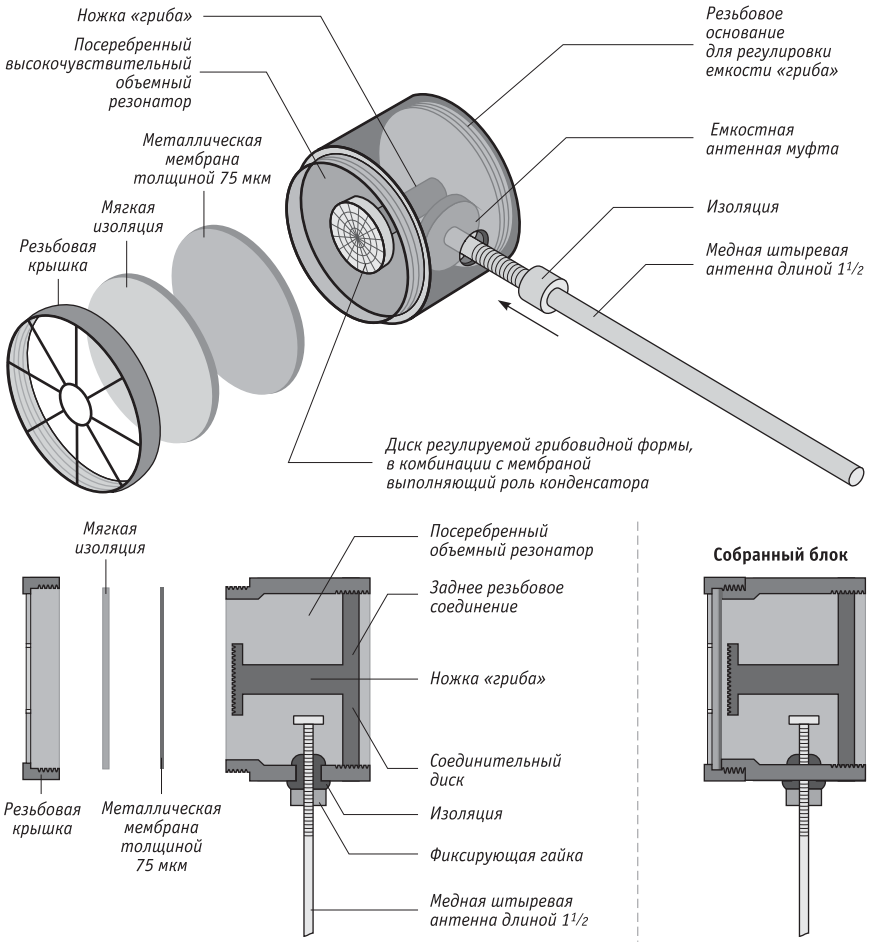


Рис. 6. ***Макет The Thing***

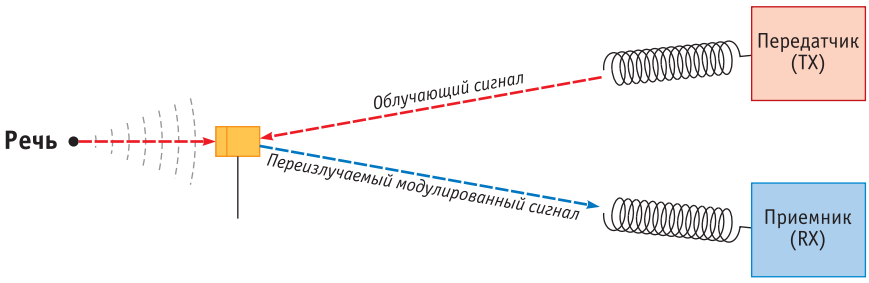
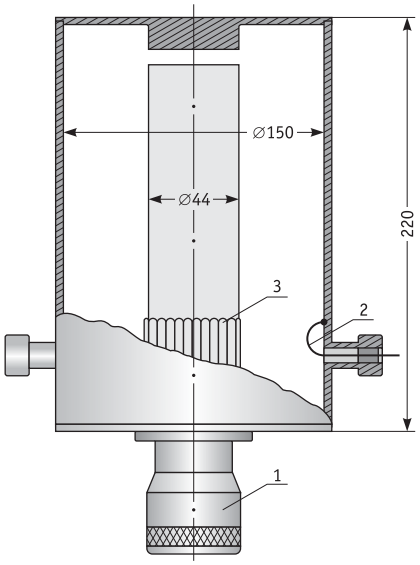


Рис. 7. ***Схема применения The Thing***



1 – микрометр, 2 – петля связи, 3 – контактные пружины

Рис. 8. ***Классический коаксиальный резонатор для измерения свойств диэлектриков на частотах 250–300 МГц [3, 6]***

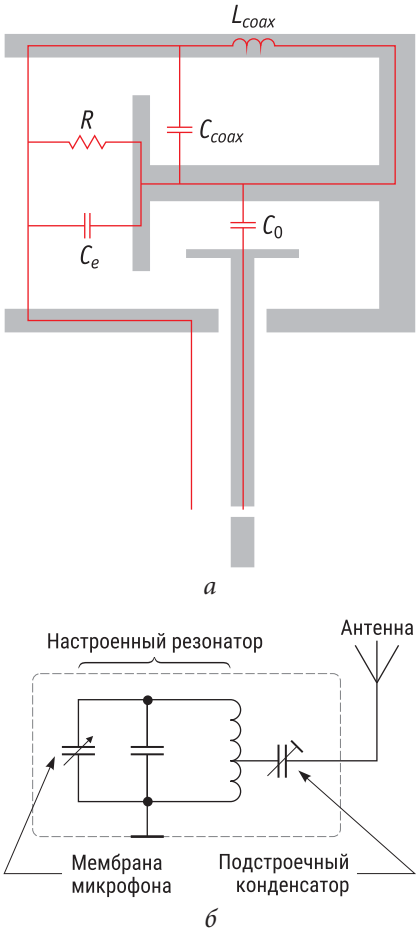


Рис. 9. ***Поперечное сечение преобразователя и аналогия электрической цепи (а), а также упрощенная электрическая схема (б)***

зонатор был использован в качестве умножителя частоты [3].

Некоторые причины сложности точного определения параметров ЗУ

Еще раз напомним, что принципы работы «Златоуста» в 1940-е годы были хорошо знакомы специалистам в области радиотехники. Так, в июле 1949 года было оформлено авторское свидетельство на изобретение «Применение полого электромагнитного резонатора (эндовибратора) в качестве преобразователя (датчика) малых механических величин (перемещений) в электротехнике» [16]. Резонансные методы с успехом использовались для измерений параметров газов, обладающих малыми значениями проницаемости и потерь, а также для исследования жидких веществ при очень малых количествах материала, необходимого для исследования. Например, метод измерения свойств твердых веществ (измерения производятся на частотах 250–300 МГц) основан на использовании коаксиального резонатора с торцевым зазором. Высота торцевого зазора резонатора (рис. 8) может изменяться при помощи микрометрического винта в пределах от 0 до 10 мм, что дает возможность настраивать резонатор на заданную частоту.

Приведенный на рис. 3 чертеж «Златоуста» можно представить в виде электрической схемы (колебательный контур, подключенный к штыревой антенне). Мембрана микрофона изображена в виде конденсатора переменной емкости (изменения происходят пропорционально воздействующему акустическому сигналу). С некоторыми оговорками можно рассматривать мембрану как конденсаторный микрофон (изобретен в 1916 году инженером Bell Labs Эдуардом Венте). Антенна связана с колебательным контуром через регулируемое механическое устройство, эквивалентное разделительному конденсатору.

Вид поперечного сечения преобразователя и аналогия электрической цепи приведены на рис. 9. Сам резонатор моделируется как коаксиальный резонатор с параметрами L_{coax} и C_{coax}. Диаграмма и диск на конце центрального стержня моделируются конденсатором, обозначенным C_e. Сопротивление воздуха между диафрагмой и диском моделируется резистором R. Антенна имеет емкостную связь с резонатором, причем емкость обозначается C_0. На рис. 9 эти элементы схемы накладываются поверх схемы поперечного сечения для большей наглядности. Примерно рассчитать первую резонансную частоту на первый взгляд несложно [6, 15]:

$$f_1 = 1/\{2\pi\sqrt{[L_{coax}(C_{coax}+ C_e)]}\}. \quad (2)$$

Ввиду отсутствия точных параметров «Златоуста» расчеты независимых исследователей дают самые разные значения первой резонансной частоты.

Схема предельно простая, а реализация заслуживает уважения. На рис. 10 показан принцип амплитудной модуляции ВЧ-сигнала при изменении емкости воздушного микрофона (мембраны) [17].

Ключевым вопросом, определяющим требуемую мощность облучения, является индекс модуляции отраженного сигнала. Индекс зависит от параметров резонатора и частоты зондирующего сигнала.

Полосой пропускания контура называют полосу частот, в пределах которой ток в контуре уменьшается не более чем в $\sqrt{2}$ раз по сравнению с током при резонансе (в 2 раза по мощности). Иначе говоря, полосой пропускания контура называют полосу частот, в пределах которой контурный ток составляет 0,7 или больше от тока при резонансе (0,5 – по мощности). На рис. 11 изображена резонансная кривая колебательного контура.

Полоса пропускания этого контура равна

$$\Delta f = f_{макс} - f_{мин}. \quad (3)$$

Ширина полосы пропускания прямо пропорциональна резонансной частоте и обратно пропорциональна добротности контура:

$$f = f_0/Q, \quad (4)$$

причем Q определяется из выражения

$$Q = 1/[2\pi f_0 CR] = 2\pi f_0 LR, \qquad (5)$$

где C – емкость, L – индуктивность, R – активное сопротивление колебательного контура.

С учетом выражений из [2] можно рассчитать индекс АМ-модуляции при правильной настройке зондирующего сигнала и резонансной частоты контура (см. врезку), и в более привычном виде

$$M_{ам}[\%] = m_{AM} \times 100. \qquad (7)$$

В таблице приведены примерные значения индекса модуляции для объемного резонатора с резонансной частотой 330 МГц и 1000 МГц.

С некоторой натяжкой можно отметить, что обнаружить наличие модуляции зондирующего сигнала во время рутинного радиоконтроля можно при значении индекса модуляции порядка 10^{-3}–10^{-2}. Идентифицировать речевой сигнал на стандартном радиоприемном оборудовании получится в случае превышения индекса модуляции величин 10^{-2}–10^{-1}. При $Q > 1000$ возможно вести разведку на значительном расстоянии. Достоинством объемного резонатора являются изначально высокая добротность, полное экранирование, жесткость и прочность конструкции, небольшие размеры. Ясно, что для повышения индекса модуляции частоту зондирования при использовании объемного резонатора надо по возможности снижать. С другой стороны, с ростом частоты уменьшаются геометрические размеры. То есть, в любом случае требовался компромисс.

Заслугой нашего выдающегося инженера Л. С. Термена было принятие решения об использовании известного эффекта для ведения акустической разведки, рациональный выбор параметров объемного резонатора и частоты облучения. Приведем в качестве примера результаты исследования специалистами ЦРУ влияния величины торцевого зазора на эффективность работы РЛСАР. На рис. 12 приведена экспериментально полученная зависимость сигнала на выходе приемника РЛСАР от расстояния до мембраны.

За отметку «0» по оси абсцисс взята величина зазора мембраны 125 мкм, далее зазор увеличивался с шагом ≈2 мкм. Очевидно существенное влияние (>30 дБ) данного параметра на результаты применения закладочного устройства. Мы знаем, что величина торцевого зазора в «Златоусте» составляла 230 или 250 мкм. Но при этом эксперименте американцы использовали зондирующую частоту 1000 МГц.

Небольшое вмешательство в параметры ЗУ резко меняло предварительную тщательную настройку устройства. Большое количество

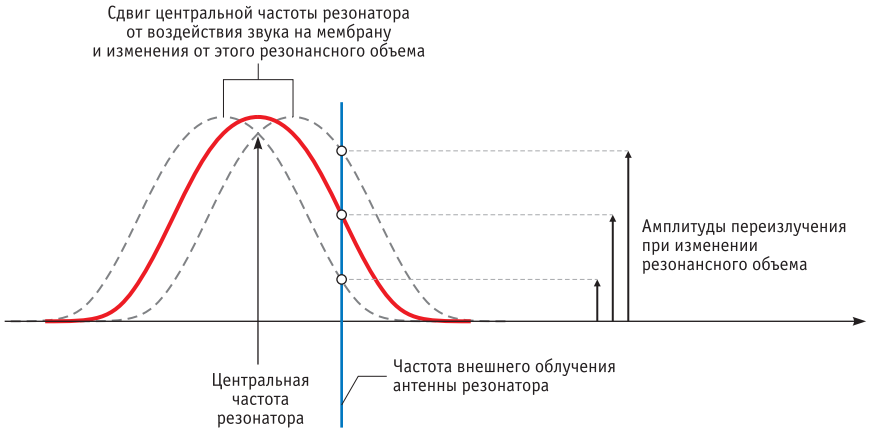


Рис. 10. ***Амплитудная модуляция ВЧ-сигнала при изменении емкости воздушного микрофона (мембраны)***

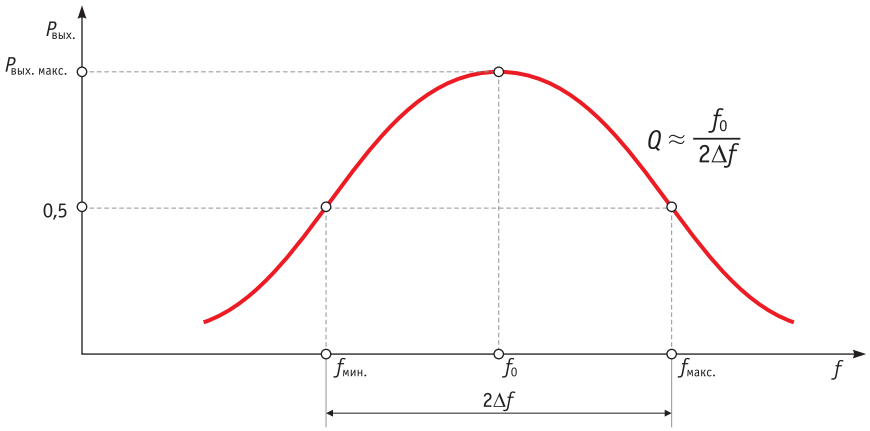


Рис. 11. ***Резонансная кривая колебательного контура***

Врезка

$$m_{AM} = 1 - \{1/\sqrt{(1 + 4 \times 10^{-4}(Q/f_{рез}[МГц])^2)}\}, \qquad (6)$$

где Q – добротность резонатора.

Таблица. ***Значения индекса модуляции $M_{ам}$ (%) с резонансной частотой 330 МГц и 1000 МГц***

Добротность ОР	Частота, МГц	
	330	1000
50	$4{,}6 \times 10^{-4}$	5×10^{-5}
500	$4{,}6 \times 10^{-2}$	5×10^{-3}
1000	$3{,}7 \times 10^{-1}$	2×10^{-2}
5000	4,3	0,5
10 000	15	1,9
50 000	69	30

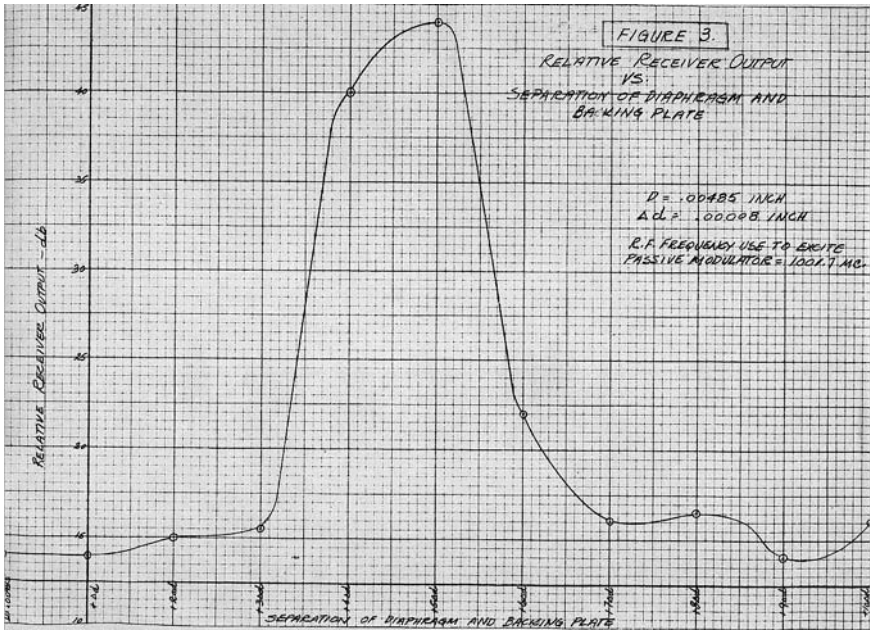


Рис. 12. ***Зависимость сигнала на выходе приемника РЛСАР от величины торцевого зазора [18]***

собственных резонансных частот позволяло получать многочисленные отклики, правда, с разными уровнями значения индекса модуляции. Из-за использования относительно маломощных лабораторных генераторов исследователи из ФБР, ЦРУ, МИ-5 не могли однозначно определить истинную частоту, которая позволяла достичь максимальной дальности работы устройства, да и времени у них было мало, так как «давило» начальство.

Итак, из имеющихся данных можно сделать следующие выводы:

- принцип работы «Златоуста» определен правильно всеми экспертами (хотя эндовибраторы ранее никогда не применялись в качестве прослушивающих устройств, их свойства были известны);
- схема построения системы в треугольнике «передатчик – закладочное устройство – приемник» определена правильно;
- частоту эксперты определяли по длине антенны, соответственно, получили разные значения: от 310 до 1900 МГц;
- быстро созданные аналоги дали существенный разброс по частоте;
- на многих длинах волн можно было получить отклик, убеждавший, что устройство работоспособно;
- при неправильном выборе частоты дальность заметно снижалась;
- попытки «привязать» к работе The Thing принципы нелинейной локации несколько опережали время, а потому были признаны несостоятельными. ■

ЛИТЕРАТУРА

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

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

3. The Thing. Great Seal Bug [Электронный ресурс]. – URL: https://www.cryptomuseum.com/covert/bugs/thing/index.htm (дата обращения: 18.05.2022).

4. History of the Bureau of Diplomatic Security of the United States Department of State // United States Department of State Bureau of Diplomatic Security. Global Publishing Solutions First Edition. Printed, October 2011. – 441 p.

5. Office Memorandom. June. [Электронный ресурс]. – URL: https://www.cryptomuseum.com/covert/bugs/thing/files/19520923_fbi.pdf (дата обращения: 29.05.2022).

6. Thompson C., Hu L., Remillard G., Chandra K. Analysis of a passive radio frequency excited acoustic transducer // 177th Meeting of the Acoustical Society of America, Louisville, Kentucky,13–17 May 2019. V. 36 (030001). P. 1–10.

7. Wright P. Spycatcher. The Candid Autobiography of a Senior Intelligence Officer. William Heinemann Australia, 1987.

8. Алексеенко В. Н., Мелтон К. Шпионский арсенал. История оперативной техники спецслужб. – М.: Алгоритм. – 2016. – 432 с.

9. Report in research on Easychair [Электронный ресурс]. – URL: https://www.cryptomuseum.com/covert/bugs/ec/files/19550714_cia.pdf (дата обращения: 29.05.2022).

10. Шпионское оружие: туфли, зонты и другие смертельно опасные вещи [Электронный ресурс]. – URL: https://3dnews.ru/916083/page-2.html (дата обращения: 08.07.2022).

11. Brooker G., Gomez, J. Lev Termen's Great Seal Bug Analyzed // IEEE A&E Systems Magazine, November 2013. [Электронный ресурс]. – URL: https://www.academia.edu/7275923/Lev_Termens_Great_Seal_bug_analyzed/ (дата обращения: 30.05.2022).

12. Pursglove D. How Russia Spy Radio Works // American Electronics Illustrated. – January 1962. P. 89–91.

13. J. Edgar Hoover to John W. Ford. Drawing and Photographs, Russian Resonant Cavity Microphone FBI. 1 December 1952 // Released to a selected group on 4 December 1952. Declassified and approved for release by the FBI on 24 April 2019 persuant to E.O. 13526.

14. Как СССР шпионил за США [Электронный ресурс]. – URL: https://www.popmech.ru/weapon/169641-gerbssha-s-unikalnoy-shpionskoy-nachinkoy/ (дата обращения: 29.05.2022).

15. Thompson C., Jallah J., Chandra, K. Analysis of a Passive Radio Frequency Excited Acoustic Transducer, CACT Technical Teport, summer 2018. [Электронный ресурс]. – URL: https://www.semanticscholar.org/paper/Analysis-of-a-passive-radio-frequency-excited-Thompson-Jallah/4268824a9193d8b08e2a500dbc3bb 5ff719dd0e9/ (дата обращения: 02.07.2022).

16. Прохоров В. П., Дерюгин Л. К., Никитина А. М. Применение пологого электромагнитного резонатора (эндовибратора) в качестве преобразователя (датчика) // Патент № SU 86284 A1. Заявка от 23 июня 1949 г. за № 399498.

17. Гениальное – просто: «жучок» Льва Термена [Электронный ресурс]. – URL: http://www.433175.ru/uploads/posts/2016-02/1454673092_sx2.jpg (дата обращения: 02.07.2022).

18. Report in research on Easychair [Электронный ресурс]. – URL: https://www.cryptomuseum.com/ covert/bugs/ec/files/19550714_cia.pdf (дата обращения: 30.05.2022).

СОДЕРЖАНИЕ ЖУРНАЛА ЗА 2022 ГОД

№ 1 (103)

ТЕМА НОМЕРА

Технические каналы утечки информации: проблемы и решения

КАТАЛОГ

Средства противодействия экономическому шпионажу

№ 2 (104)

ТЕМА НОМЕРА

Безопасность киберфизических систем

Безопасность компьютерных систем

Спецтехника

Защита информации в технических каналах

№ 3 (105)

Защита информации в технических каналах

ТЕМА НОМЕРА

Кибервызовы сегодняшнего дня

Безопасность компьютерных систем

Современные технологии

№ 4 (106)

№ 5 (107)

№ 6 (108)

ВАС ПОДСЛУШИВАЮТ? Звоните нам!

СПЕЦИАЛИЗИРОВАННЫЙ ХОЛДИНГ
ЛАБОРАТОРИЯ ППШ

199178, Санкт-Петербург, наб. реки Смоленки, д. 25
+7 (812) 702-73-83
e-mail: lab@pps.ru, http://www.pps.ru

Информационно-методический журнал

INSIDE
ЗАЩИТА ИНФОРМАЦИИ

Подписная кампания

2023

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, 2023 г.) – **3840** руб.
Годовая подписка (№ 1–6, 2023 г.) – **7680** руб.

Подписка на электронную версию журнала

Период подписки: весь 2023 год – **7680** руб.
Электронная версия выполнена в формате *.pdf

Специальное предложение: печатная + электронная версии – **9984** руб. Период подписки: весь 2023 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 2015–2022 годы на CD

Полные тексты всех статей с диаграммами, таблицами, графиками, иллюстрациями.

Ознакомиться с содержанием CD и оформить заказ можно в интернет-магазине на нашем сайте: http://www.insidezi.ru/.

Стоимость с учетом доставки заказной бандеролью – **9376** руб.

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/