МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики» (МТУСИ)

Федеральное учебно-методическое объединение в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ)

Всероссийская научная школа-семинар

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ МЕТОДОВ И ТЕХНОЛОГИЙ ЗАЩИТЫ ИНФОРМАЦИИ

СБОРНИК

30 ноября 2021 г.

Москва
2021

Всероссийская научная школа-семинар

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ МЕТОДОВ И ТЕХНОЛОГИЙ ЗАЩИТЫ ИНФОРМАЦИИ

* * *

ДАТА И МЕСТО ПРОВЕДЕНИЯ

30 ноября 2021 года

Московский технический университет связи и информатики (МТУСИ),
г. Москва, ул. Авиамоторная, д. 8а

* * *

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

Леохин Ю.Л., д.т.н., профессор, проректор по научной работе МТУСИ (председатель);

Белов Е.Б., заместитель председателя ФУМО ВО ИБ (заместитель председателя);

Лось В.П., д.в.н., профессор, президент МОО «Ассоциация защиты информации»;

Новиков С.Н., д.т.н., доцент, заведующий кафедрой «Безопасность и управление в телекоммуникациях» СибГУТИ;

Киреева Н.В., к.т.н., доцент, декан факультета «Телекоммуникации и радиотехника» ПГУТИ;

Красов А.В., к.т.н., доцент, заведующий кафедрой «Защищенные системы связи» СПбГУТ;

Безумнов Д.Н., старший преподаватель кафедры «Интеллектуальные системы в управлении и автоматизации» МТУСИ (секретарь).

ОГЛАВЛЕНИЕ

Смирнов С.И.
Российский технологический университет – МИРЭА,
аспирант,
smirnov_si@mirea.ru

ПОДХОД К ОБНАРУЖЕНИЮ ВРЕДОНОСНОЙ АУТЕНТИФИКАЦИОННОЙ АКТИВНОСТИ ЗЛОУМЫШЛЕННИКА ПРИ РАССЛЕДОВАНИИ КИБЕРИНЦИДЕНТА

Проблеме обнаружения вредоносных действий злоумышленника при расследовании киберинцидентов посвящено большое количество работ как отечественных ученых (П.Д. Зегжды, Д.П. Зегжды [1], М.А. Еремеева, А.Г. Ломако [2], И.В. Котенко, С.А. Петренко, В.А. Овчарова [3], И.Б. Саенко [4]), так и зарубежных (Prasanta Kumar Sahoo, R.K. Chottray, S.Pattnaiak, Julius Barath, Mart Meijerink, Tim Niklas Witte и др.).

В целом анализ текущего состояния обнаружения вредоносных воздействий злоумышленника при проведении расследования киберинцидентов [5] показывает, что возможности существующих программных средств не удовлетворяют требованиям практики. Существующие программные средства являются лишь отображением событий безопасности, которых может быть большое количество. Примерами данных программных средств являются: Event Viewer, Event Log Explorer. Что касается математической основы анализа событий в SIEM-системах, то стоит отметить наличие лишь созданных правил корреляции для событий безопасности.

Следует отметить, что в настоящее время необходим поиск новых научно-технических решений, позволяющих повысить оперативность обнаружения вредоносного воздействия злоумышленника в быстро

меняющихся условиях уровня информационной безопасности в сети. Принципиальной особенностью современных расследований киберинцидентов является большое количество исходных данных – событий безопасности в журналах домена.

Вне зависимости от сценария целевых атак после получения первоначального доступа злоумышленник применяет техники горизонтального перемещения, необходимые для получения прав администратора домена. К таким техникам относят: Pass-the-Hash, Pass-the-Ticket и др. Применение данных техник непременно оставляет следы с течением времени, обнаруживать которые возможно с помощью интеллектуального анализа событий безопасности ОС Windows:

- 4624 – учетная запись была успешно авторизована в системе;
- 4625 – учетная запись не смогла авторизоваться в системе;
- 4768 – запрошен билет проверки подлинности Kerberos (TGT);
- 4769 – запрошен билет службы Kerberos (TGS);
- 4776 – контроллер домена попытался проверить учетные данные пользователя по протоколу NTLM.

Основная идея исследования заключается в анализе аутентификационной активности пользователей ОС Windows в корпоративной сети различными моделями машинного обучения временных рядов.

В области интеллектуального анализа данных наблюдается повышенный интерес к проблемам обнаружения редких событий (статистических выбросов) и мониторинга активности (в частности, обнаружения точек изменения) на основе нестационарных источников данных (нестационарных временных рядов), то есть источников, природа которых может изменяться со временем. Для определения статистического

поведения данных временных рядов с целью выявления выбросов и точек изменения используется модель авторегрессии (AP).

Исследуемая последовательность данных, например событий журнала безопасности Security.evtx, образует временной ряд, поэтому в качестве математического аппарата для исследований автором проекта предлагается использовать алгоритм Change Finder, основанный на модели авторегрессии (AP). Данный алгоритм был описан в работе [6]. Модель AP является одной из наиболее типичных моделей для представления временных рядов.

Прикладной значимостью проекта является применение данного алгоритма в методике, нацеленной на повышение оперативности для выявления вредоносной активности злоумышленника при расследовании инцидентов информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Зегжда, Д. П. Управление динамической инфраструктурой сложных систем в условиях целенаправленных кибератак / Д. П. Зегжда, Д. С. Лаврова, Е. Ю. Павленко // Известия Российской академии наук. Теория и системы управления. – 2020. – № 3. – С. 50-63.
2. Калинин, В.Н. Расследование ИБ-инцидентов с использованием профилирования поведения динамических сетевых объектов / В. Н. Калинин, А. Г. Ломако, В. А. Овчаров, С. А. Петренко // Защита информации. Инсайд. – 2018. – № 3(81). – С. 58-67.
3. Овчаров, В. А. Расследование компьютерных инцидентов на основе идентификации дискретных событий информационной безопасности и обратного анализа по конечным исходам / В. А. Овчаров, П. А. Романов // Труды Военно-космической академии имени А.Ф.Можайского. – 2015. – № 648. – С. 84-89.

4. Саенко, И.Б. Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры / И. Б. Саенко, О. С. Лаута, М. А. Карпов, А. М. Крибель // Электросвязь. – 2021. – № 1. – С. 36-44.
5. Смирнов, С.И. Анализ техник и инструментов, используемых злоумышленником при горизонтальном перемещении в корпоративной сети / С. И. Смирнов, М. А. Еремеев, И. Е. Горбачев [и др.] // Защита информации. Инсайд. – 2021. – № 1(97). – С. 58-61.
6. Takuma Iwata, Kohei Nakamura, Yuta Tokusashi, and Hiroki Matsutani Accelerating. 2018. Online Change-Point Detection Algorithm using 10GbE FPGA NIC [In book: Euro-Par,: Parallel Processing Workshops]. doi: 10.1007/978-3-030-10549-5_40.

Плугатарев А.В.

Юго-Западный государственный университет,

аспирант,

aplugatarev@bk.ru

МЕТОДЫ И АЛГОРИТМЫ ИСПОЛЬЗОВАНИЯ МЕТАДАННЫХ ДЛЯ ИСПРАВЛЕНИЯ ОШИБОК АУТЕНТИФИКАЦИИ ПРИ СЕТЕВОМ ВЗАИМОДЕЙСТВИИ

Задачи, связанные с методами защиты информации от несанкционированного доступа — важная часть исследований информационных наук, так как архитектуры современных информационных систем требуют от пользователей процедуру проверки подлинности — процесса аутентификации. Механизмы аутентификации требуют использования ресурсов информационной системы, которые по своей сути не направлены на непосредственное выполнение задач, выполняемых данной системой [1]. В зависимости от задач систем, к методам проверки подлинности выдвигаются различные требования к надёжности и ресурсным затратам. Как правило, во всех системах высокие требования к надёжности, и к экономии вычислительных ресурсов и ресурсов хранения данных. Следовательно, актуальным становится вопрос исследования, механизмов аутентификации, так как с повышением мощностей вычислительной техники и прогрессу мировой сетевой инфраструктуры, возможности злоумышленников получить несанкционированный сетевой доступ возрастают, а ресурсы систем, зачастую, ограничены, что и требует постоянных исследований в области защиты информации [2].

Таким образом, целью работы является увеличения вероятности обнаружения ошибки контроля целостности или аутентичности; уменьшения

затрат временных и аппаратных ресурсов приёмника, в рамках сетевого взаимодействия с передатчиком по ограниченному пропускной способности каналу связи; достижение наименьшей вероятности возникновения ошибки за счёт анализа метаинформации, и определения порогового значения, при котором можно считать аутентификацию успешной.

Основные положения данного исследования можно обозначить следующим образом:

1. Методы контроля аутентификации, основанные на алгоритмах анализа метаинформации коммутационных пакетов при сетевом взаимодействии, позволяют значительно снизить информационную избыточность методов контроля целостности и аутентичности, а также повысить пропускную способность канала.

2. Алгоритмы вычисления порогового значения вероятности обнаружения ошибки аутентификации, основанные на базе клеточных автоматов, а также методов машинного обучения повышают вероятность обнаружения несанкционированного доступа к информационной системе.

Вышеупомянутые методы, позволяющие обнаруживать нарушения аутентичности или целостности информации, основаны на анализе таких метаданных коммутационных пакетов, как например, время, порядковый номер и различных поведенческих особенностей, и вычислении порогового значения на основе данных параметров.

Главной задачей исследования можно обозначить исследование зависимости вероятности обнаружения возникновения ошибки контроля целостности и аутентичности информационного сигнала от методов вычисления порогового доверительного значения обнаружения ошибки, пропускной способности коммутационного канала, степени загруженности информационной системы, способов передачи данных, а также разработку

методов выделения признаков успешной аутентификации передатчика на приёмнике

В работе используется возможность использования такого параметра, как время поступления информационного пакета в приёмник для снижения вероятности ошибки идентификации источника информационного пакета. Численные значения времени поступления информационного пакета анализируются на предмет наличия резких отклонений прогнозируемого численного значения времени поступления единицы сетевого взаимодействия от реального. Таким образом, отклонение времени поступления какого-либо пакета от ожидаемого на определённое значение является признаком того, что он выдан не данным источником [3].

Результатом исследования является создание способа расчёта вероятности ошибок аутентификации, которые основаны на алгоритмическом анализе метаданных коммутационных пакетов сетевого взаимодействия, при помощи алгоритмов основанных на клеточных автоматах и системах машинного обучения, что в свою очередь позволит увеличить пропускную способность каналов сетевого взаимодействия, и повышение вероятности обнаружения ошибки аутентификации при использовании метаинформации, содержащейся в информационных сигналах.

СПИСОК ЛИТЕРАТУРЫ

1. Бабаш А. В. Информационная безопасность предприятия: Учебное пособие / Бабаш А. В., Баранова Е. К., Ларин Д.А. Гришина, Н.В. // - М.: Форум, 2018. - 118 с.
2. Буренин А.Н., Легков К.Е. Основные проблемы безопасности подсистем обеспечения единым временем элементов систем управления сложными организационно-техническими объектами / Буренин А.Н., Легков К.Е. // T-comm: телекоммуникации и транспорт. 2019. С. 48.

3. Таныгин М.О. / Использование метаданных для исправления ошибок аутентификации при сетевом взаимодействии. / Таныгин М.О., Алшаиа Х.Я., Хемраев Д. // В сборнике: Сборник докладов XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции "Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации" (ИНФОБЕЗОПАСНОСТЬ -2019). доклады XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции. Отв. редактор: В.И. Петренко. 2019. С. 14-18.

Симахин Е.А.
Национальный исследовательский ядерный университет «МИФИ»,
инженер 2-й категории,
EASimakhin@mephi.ru

О ПОБОЧНОМ ЭЛЕКТРОМАГНИТНОМ ИЗЛУЧЕНИИ ИНТЕРФЕЙСОВ ПЕРЕДАЧИ ДАННЫХ ЖИДКОКРИСТАЛЛИЧЕСКИХ МОНИТОРОВ

В процессе обработки информации средства вычислительной техники излучают информативные электромагнитные волны. При перехвате данного излучения существует возможность восстановления конфиденциальной информации [1]. В связи с этим появляется потенциальная угроза информационной безопасности – утечка информации по каналу побочных электромагнитных излучений и наводок. Рассматриваемый канал работает фактически в реальном масштабе времени, является пассивным, что не дает возможности владельцу информации обнаружить нарушителя. Поэтому в последние годы данному техническому каналу утечки информации уделяется пристальное внимание.

Особый интерес со стороны специалистов по технической защите информации представляют работы, связанные с анализом побочных электромагнитных излучений интерфейсов передачи данных жидкокристаллических мониторов, позволяющий оценить уязвимость объекта информатизации. Так, в 2013, в журнале «IEEE Transaction on electromagnetic compatibility» была опубликована научная статья [2], в которой говорится о сложности подхода к анализу побочных электромагнитных излучений от жидкокристаллических мониторов. Тем не менее, уже в 2014 году отечественным исследователем была предложена математическая модель и

методика оценки возможностей перехвата побочных электромагнитных излучений видеосистемы компьютера с помощью оптимального приемника [3]. В 2016 году на симпозиуме PIERS была представлена работа исследователей [4], в которой описывается исследование побочного электромагнитного излучения интерфейсов VGA и DVI. В 2020 году был предложен метод восстановления исходного сигнала видеоподсистемы монитора высокого разрешения [5]. В том же году была представлена концепция, объясняющая принципы утечки информации с использованием кабелей дифференциальных сигналов (DVI, HDMI, LVDS) [6]. Показано, что излучения от дисплеев, использующих дифференциальные сигнальные кабели, не только модулируются по амплитуде, но и по частоте, что увеличивает возможный набор алгоритмических инструментов злоумышленников. Таким образом, построение системы защиты информации от утечки по каналу побочных электромагнитных излучений и наводок на объектах информатизации является актуальным.

В настоящий момент для обеспечения информационной безопасности, гарантирующей защиту интересов личности, бизнеса и государства, а также формирования комплексной системы защиты проводится аттестация объектов информатизации. Одним из перечня требуемых мероприятий, проводимых в ходе аттестации специалистами в области технической защиты информации, является анализ побочных электромагнитных излучений интерфейсов передачи данных средств вычислительной техники, в частности жидкокристаллических мониторов. С учетом сложности и, как следствие, большими временными затратами, выполнение такого вида работ требует не только квалифицированных специалистов в области информационной безопасности, но и обеспечение автоматизации технического процесса, а также соблюдения метрологической точности. Особенностью анализа интерфейсов передачи данных жидкокристаллических мониторов

относительно интерфейсов других устройств является наличие нескольких компонентов, побочное излучение которых приводит к потенциальной утечке конфиденциальной информации. Вследствие этого, при проведении лабораторных исследований специалистам требуется проводить анализ отдельно каждого из компонентов, что на данный момент возможно только ручным эмпирическим методом.

Таким образом, для обеспечения требуемой точности и полноты результатов лабораторных исследований при условии уменьшения трудозатрат необходимо разработать автоматизированный метод оценки побочных электромагнитных излучений интерфейсов передачи данных жидкокристаллических мониторов. Как следствие, результатом исследования является разработка учебного материала в виде лабораторного практикума и, при необходимости, дополнительных требований к пассивным и активным средствам защиты информации и уточнение методик сертификационных испытаний их программного обеспечения.

СПИСОК ЛИТЕРАТУРЫ

1. Wang L. Research on the compromising electromagnetic emanation from digital signals / L. Wang, B. Yu // Proceedings of “International Conference on Automatic Control and Artificial Intelligence” — 2012 — 1761-1764.
2. Kuhn. M. G. Compromising emanations of LCD TV sets / M. G. Kuhn. // IEEE Transaction on electromagnetic compatibility — 2013 — vol. 55, no.3 — 564-570.
3. Horev A.A. Evaluation of the possibility of detection side compromising electromagnetic emanations video PC / A.A. Horev // Proceedings of TUSUR University — 2014 — no.2 — 207-213.

4. Nowosielski L. Compromising Emanations from VGA and DVI Interface / L. Nowosielski, R. Przesmyckil, M. Nowosielski // Proceedings of “Progress In Electromagnetic Research Symposium (PIERS)” — 2016 — 1024-1028.
5. De Meulemeester P. A Quantitative Approach to Eavesdrop Video Display Systems Exploiting Multiple Electromagnetic Leakage Channels / P. De Meulemeester, B. Scheers, G. A. E. Vandenbosch // IEEE Transaction on electromagnetic compatibility — vol. 62, no. 3 — 2020 — 2376-2385.
6. De Meulemeester P. Differential signaling compromises video information security through AM and FM leakage emissions / P. De Meulemeester, B. Scheers, G. A. E. Vandenbosch // IEEE Transaction on electromagnetic compatibility — vol. 62, no. 6 — 2020 — 2376-2385.

Павлов А.С.
Северо-Кавказский федеральный университет,
инженер-лаборант,
losde5530@gmail.com

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОЦЕССА МАСШТАБИРОВАНИЯ ЧИСЛЕННОСТИ АГЕНТОВ В РОЕВЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМАХ

Переход к передовым цифровым, интеллектуальным производственным технологиям актуализирует направление развития роевых робототехнических систем (РРТС) как вида групповой робототехники. РРТС предназначены для решения широкого спектра задач: мониторинг и ликвидация чрезвычайных ситуаций, спасательные операции, подводные исследования, сельскохозяйственные работы, разведывательные операции, а также многие другие [1].

В англоязычных публикациях для определения групповой робототехники преимущественно используется термин мульти роботизированные системы (МРС, от англ. «Multi-robot system»), включающий в себя множество возможных способов организации групп робототехнических средств. РРТС является частным случаем МРС, которая имеет следующие особенности:

- идентичное структурно-функциональное устройство роботов (далее «агентов»), включающее бортовые датчики и сенсоры с ограниченной дальностью действия и низко-производительные вычислительные устройства, независимо от конкретной аппаратной реализации;

- полная децентрализация взаимодействия агентов на основе самоорганизации, из чего следует отсутствие центрального узла (агента-координатора);

- отсутствие полной информации обо всех агентах РРТС ввиду вышеперечисленных ограничений, из чего следует отсутствие идентификаторов у агентов (при этом максимальная численность агентов не лимитирована).

Одним из ключевых преимуществ использования РРТС является возможность масштабирования количества агентов при увеличении сложности задания (например, увеличение площади территории, на которой необходимо осуществить мониторинг или разведку для сбора данных) [2]. Дополнительно привлеченные агенты могут быть направлены как из управляющего центра, так и переназначены оператором в ходе выполнения собственного задания с меньшим приоритетом важности. При этом актуальным вопросом обеспечения информационной безопасности РРТС становится аутентификация и авторизация новых агентов РРТС. Это обусловлено тем фактом, что достаточно лишь одного вредоносного агента для того, чтобы нарушить функционирование РРТС [3].

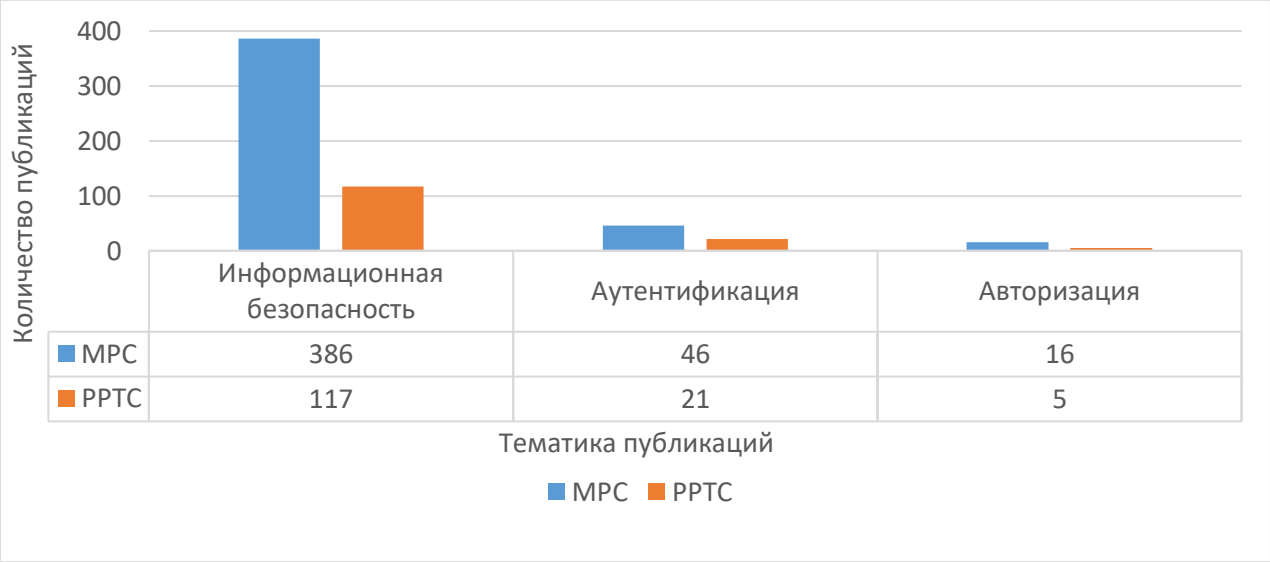

Рис. 1. Количество публикаций в базе Scopus по данной тематике

В силу перечисленных особенностей РРТС применение известных методов и алгоритмов аутентификации и авторизации невозможно или существенно ограничено без их модификации. Количество публикаций по тематике данной работы в базе Scopus представлено на Рис. 1 (в сравнении с публикациями, направленными на обеспечение информационной безопасности в МРС).

Разница в количестве публикаций по смежным темам вызвана ограничениями, которые накладываются в случае исследований, направленных на обеспечение информационной безопасности в РРТС. Данный факт, а также результаты аналитических исследований авторов работ [3-6] подтверждают важность и своевременность решения задачи обеспечения информационной безопасности в РРТС.

СПИСОК ЛИТЕРАТУРЫ

1. Zakiev, A. Swarm Robotics: Remarks on Terminology and Classification / A. Zakiev, T. Tsoy, E. Magid // Interactive Collaborative Robotics (ICR 2018). — 2018. — P. 291-300. DOI:10.1007/978-3-319-99582-3_30.
2. Petrenko, V.I. Path Planning Method in the Formation of the Configuration of a Multifunctional Modular Robot Using a Swarm Control Strategy / V.I. Petrenko, F.B. Tebueva, A.S. Pavlov, V.O. Antonov, M.S. Kochanov // 7th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2019), Advances in Intelligent Systems Research. — 2019. — Vol-166. — P. 165-170. DOI: https://doi.org/10.2991/itids-19.2019.30.
3. Sargeant, I. Review of Potential Attacks on Robotic Swarms / I. Sargeant, A. Tomlinson // Lecture Notes in Networks and Systems. — 2018. — P. 628-646. 10.1007/978-3-319-56991-8_46.

4. Higgins, F. Survey on Security Challenges for Swarm Robotics / F. Higgins, A. Tomlinson, K. Martin // Fifth International Conference on Autonomic and Autonomous Systems. — 2009. — P. 307-312. DOI:10.1109/ICAS.2009.62.
5. Vangala, A. Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective / A. Vangala, A.K. Das, N. Kumar, M. Alazab // IEEE Sensors Journal. —2020. — P. 17591-17607. DOI: 10.1109/JSEN.2020.3012294.
6. Nikander, J. Requirements for cybersecurity in agricultural communication networks / J. Nikander, O. Manninen, M. Laajalahti // Computers and Electronics in Agriculture. — 2020. — P. 1-10. DOI: 10.1016/j.compag.2020.105776.

Евсюков М.В.

Кубанский государственный технологический университет,

аспирант,

michael.evsyukov@gmail.com

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И КОНТРОЛЯ ПРИ ВЗАИМОДЕЙСТВИИ С ГОЛОСОВЫМИ АССИСТЕНТАМИ НА ОСНОВЕ ИДЕНТИФИКАЦИИ РЕЧИ ПОЛЬЗОВАТЕЛЯ

Согласно прогнозов исследовательского проекта Business Insider Intelligence, к 2022 году количество пользователей голосовых интерфейсов в США вырастет до 31% взрослого населения [1].

Востребованность голосовых платежей стимулирует банки и fintech-компании к развитию технологий искусственного интеллекта, специализированных на обработке голоса. Однако проблемы с информационной безопасностью – главное препятствие которое не позволяет, голосовым помощникам завоевать доверие банков и пользователей.

В связи с этим, целью данного исследования является совершенствование методов противодействия существующим угрозам информационной безопасности, актуальным для систем подтверждения личности по голосу.

Голосовая аутентификация – это метод биометрической аутентификации, использующий уникальные характеристики человеческого голоса в качестве признака, позволяющего подтвердить личность субъекта [2].

Голосовая аутентификация подробно изучена и демонстрирует высокую эффективность, при верификации голоса, источником которого является живой человек. Её основные преимущества – гибкость и возможность

применения для защиты смартфонов, а также устройств, подключённых к «интернету вещей» [3]. Однако её основным недостатком является уязвимость к спуфингу.

Под спуфингом понимаются действия злоумышленника, направленные на аутентификацию в системе под видом другого лица. Для противодействия спуфингу система голосовой аутентификации должна включать в себя дополнительный механизм, который называется контрмерой [4].

Концептуальная схема механизма голосовой аутентификации представлена на рисунке 1.

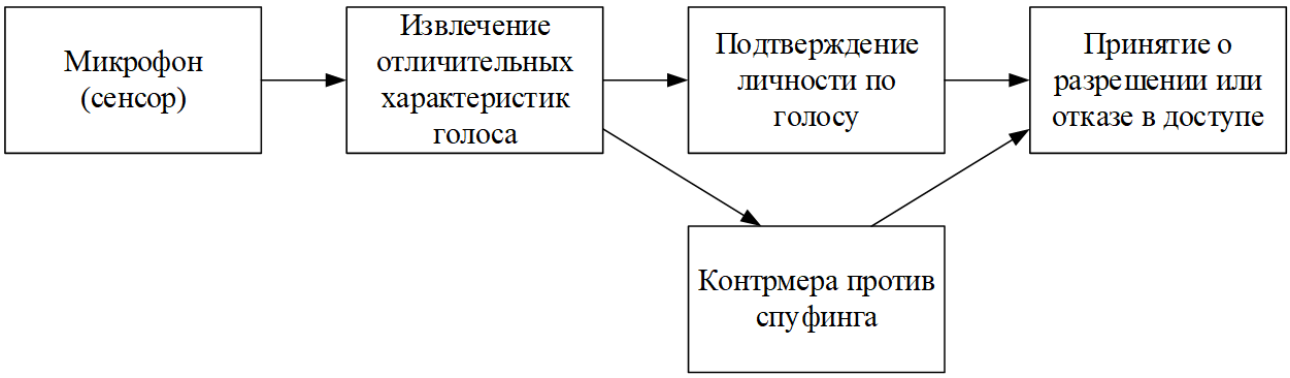

Рис. 1. Концептуальная схема современного механизма голосовой аутентификации

В ходе работы над исследованием предполагается решить следующие задачи:

- анализ современных методов голосовой аутентификации, методов спуфинга и контрмер против спуфинга;
- построение концептуальной модели системы голосовой аутентификации;
- математическое описание алгоритма работы системы голосовой аутентификации, обеспечивающего эффективное распознавание личности по голосу и противодействие спуфингу;

- разработка и тестирование программной системы голосовой аутентификации, обеспечивающей интегрированную защиту от современных методов спуфинга;
- апробация и экспериментальные исследования разработанного математического, алгоритмического и программного обеспечения системы голосовой аутентификации.

Данное исследование содержит следующие признаки научной новизны.

Во-первых, научная новизна исследования заключается разработке интегрированного средства голосовой аутентификации, которое реализует как распознавание личности по голосу, так и комплекс мер защиты от спуфинга. На данный момент большинство исследований направлены либо на антиспуфинг, либо на распознавание по голосу, в то время как в данном исследовании предлагается интегрированный подход.

Во-вторых, разрабатываемая в рамках исследования программная система ориентирована не на одноразовую, а на непрерывную аутентифкацию при взаимодействии с голосовыми помощниками.

В-третьих, в рамках работы планируется провести исследование эффективность применения различных контрмер против спуфинг-атак.

СПИСОК ЛИТЕРАТУРЫ

1. Dyke, D.V. Soon nearly a third of US consumers will regularly make payments with their voice [Электронный ресурс]. — Режим доступа: https://www.businessinsider.com/the-voice-payments-report-2017-6?r=US&IR=T.
2. Ravika, N. An Overview of Automatic Speaker Verification System / N. Ravika // Intelligent Computing and Information and Communication. – 2018. – С. 603-610.

3. Путято, М.М. Исследование возможности совершенствования кибербезопасности инфраструктуры интернета вещей на основе интеграции биометрических методов аутентификации / М.М. Путято, А.С. Макарян // Информационные системы и технологии в моделировании и управлении. Сборник трудов V Международной научно-практической конференции. – 2020. – С. 267-270.
4. El-Abed, M. Evaluation of Biometric Systems / M. El-Abed, C. Charrier // New Trends and Developments in Biometrics. – 2012. – С. 149-169.

Егорова А.О.
Ростовский государственный экономический университет (РИНХ),
аспирант,
anastasya-olegovna.kalita@yandex.ru

РАЗРАБОТКА МОДЕЛИ АДАПТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Тенденция последних десятилетий заключается в частичном или полном исключении человека из большинства процессов. Человеко-машинные комплексы на данный момент являются наиболее распространенной и продуктивной моделью осуществления деятельности. Данное направление наиболее актуально для систем, которые несут потенциальную и реальную угрозу здоровью и жизни человека или системы, угрозой для которых является человек.

Так, служба безопасности IBM Managed Security Services в отчёте «IBM Security Services 2014 Cyber Security Intelligence Index» на основании статистики, собранной в 2013 году по инцидентам в компьютерных сетях около 1000 клиентов из 133 стран, показывает, что подавляющее число инцидентов начинается с человеческой ошибки [1].

Целью данной работы является разработка и реализация модели адаптивной системы защиты информации от утечки по техническим каналам.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Рассмотреть существующие исследования в области построения адаптивных систем защиты информации, проанализировать актуальные разработки в данной области [2,3].

2. Произвести разработку и построение модели функционирования адаптивной системы защиты информации.

3. Реализовать разработанную модель в виде аппаратно-программного комплекса адаптивной защиты информации.

4. Произвести испытания и сбор данных о функционировании разработанного средства.

Объектом исследования являются системы защиты информации от утечки по техническим каналам.

Предмет исследования — методы и средства построения адаптивных систем защиты информации от утечки по техническим каналам.

Научная новизна работы заключается в следующем:

1. Впервые принципы адаптивного управления были применены в защите информации от утечки по техническим каналам.

2. Разработанная модель адаптивной системы защиты информации отличается от существующих более высокой степенью универсальности по отношению к разнообразию информационных систем.

3. Разработанный программно-аппаратный комплекс позволяет обеспечивать высокий уровень защиты от утечки по техническим каналам утечки информации.

Теоретическая значимость представленной работы состоит в развитии методов построения средств и систем защиты информации от утечки по техническим каналам с использованием алгоритмов адаптивного управления.

Практическая значимость полученных в работе результатов заключается в том, что разработанная модель и её программно-аппаратная реализация могут быть использованы для автоматизации процессов защиты информации в физических полях разной природы в информационных системах.

Данная работа соответствует следующим областям исследования:

1. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем.

2. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Таким образом, планируемым результатом для данной работы является аппаратно-программный комплекс, позволяющий производить адаптивную защиту информации от утечки по техническим каналам, используемый как средство активной защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Человеческий фактор — причина 95% инцидентов ИБ [Электронный ресурс]. — Режим доступа : https://xakep.ru/2014/06/19/62661.
2. Калита, А. О. Основы организации адаптивных систем защиты информации / А. О. Калита, М. И. Ожиганова, Е. Н. Тищенко // НБИ технологии. – 2019. – Т. 13. – № 1. – С. 11-15. – DOI 10.15688/NBIT.jvolsu.2019.1.2.
3. Ожиганова, М. И. Построение адаптивных систем защиты информации / М. И. Ожиганова, А. О. Калита, Е. Н. Тищенко // НБИ технологии. – 2019. – Т. 13. – № 4. – С. 12-21. – DOI 10.15688/NBIT.jvolsu.2019.4.2.

Путято М.М.
Кубанский государственный технологический университет,
доцент, кандидат технических наук,
putyato.m@gmail.com

РАЗРАБОТКА ТЕОРЕТИЧЕСКИХ И МЕТОДОЛОГИЧЕСКИХ ОСНОВ ПОСТРОЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ РАСПРЕДЕЛЕННЫХ СИСТЕМ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ

Проблемное поле, в которое входят вопросы обеспечения кибербезопасности, формирования защищенного киберпространства, а также различного класса системы детектирования, упреждения, предотвращения, пресечения и противодействия кибератакам и анализа новых киберугроз формируется в течение последних лет. Такие ведущие отечественные и зарубежные ученые как Котенко И. В., Чечулин А. А., Петренко С. А., Белов Е. Б., Калинин М. О., Бородакий Ю. В., Ревенков П. В., Бердюгин А. А., Зегжда Д. П., Лаврова Д. С., Лахно В. А., Лаута О. С., Промыслов В. Г., Дойникова Е. В., Васильев В. И., Соколов С. С., Зегжда П. Д., Максимов Р. В., Макаревич О. Б., Назаренко М. А., Воропай Н. И.,JulianJang-Jaccard, DanCraigen, PeterWarrenSinger, FedericoCalzolari, AthanasiosVasilakos, Yuguang "Michael" Fang, AngelosD. Keromytis, MerrillWarkentin, WillySusilo, MuhammadKhurramKhan, JosepDomingo-Ferrer, DavidDeRoure, DimitrisA. Gritzalis, AliGhorbani затрагивают основные фундаментальные вопросы, которые подтверждают свою актуальность каждый день [1, 2]:

1. Разработка новых методов детектирования и анализа перспективных кибернетических угроз в системах различного класса, в том числе в динамических сетях передачи данных (VANET, FANET, MARINET, MANET, WSN) и в киберфизических системах.

2. Исследование методов и методик выявления и противодействия кибератакам в автоматизированных системах, в том числе динамических инфраструктур сложных систем.

3. Формирование аналитического и математического моделирования для прогнозирования векторов кибератак, моделирования сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам.

4. Исследование теоретических подходов к формированию методологии кибербезопасности, в том числе функционально-семантических моделей кибербезопасности, позволяющих формализовать требования конфиденциальности, целостности и доступности, создания архитектуры агентно-ориентированного моделирования киберфизических систем , методики оценки эффективности защиты информационно-телекоммуникационной сети в условиях таргетированных кибернетических атак, современных средств и методов мониторинга и управления инцидентами комплексной безопасности систем различного класса, средств управления информационными потоками и разграничения доступа к ним и средства создания доверенной среды, методик визуализации метрик кибербезопасности, синтеза архитектуры кибербезопасности для систем управления.

Процесс цифровизации предполагает, что к данным может обращаться любой процесс или система. Поэтому подтверждение и поддержка легитимности доступа и защиты современной архитектурой ИБ, с классическим подходом к реализации системы защиты, становятся все более затруднительными.

Согласно экспертным оценкам доля киберугроз в общей массе угроз информационной безопасности будет неуклонно расти. Особую опасность представляет деперимetризация и размытие границ объектов защиты, которые

являются основой использования классических моделей информационной безопасности. В связи с этим традиционные подходы к построению систем информационной безопасности теряют свою эффективность. Данные обстоятельства требуют постановки новых целей и задач, а также выработки новых решений и способов противодействия постоянно эволюционирующим киберугрозам. Необходимо четко представлять структуру и взаимосвязи компонентов киберпространства, что позволит обеспечить выработку подходов к достижению необходимого уровня кибербезопасности каждого из элементов иерархической системы кибернетического пространства и интегральной оценки кибербезопасности в целом.

Решением поставленных задач является создание адаптивной комплексной системы обеспечения безопасности, как общая платформы обеспечит своевременный мониторинг, контекст и возможности управления в различных ситуациях (Рис. 1) [3, 4].

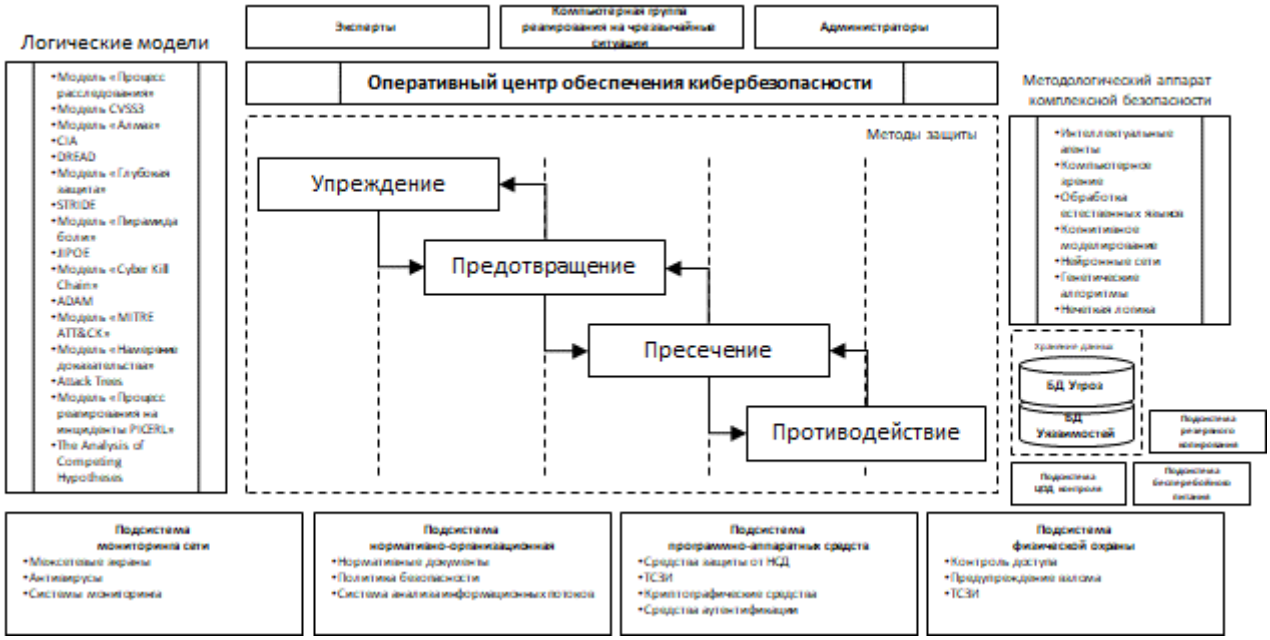

Рис. 1. Структурная модель реализации адаптивной защиты оперативного центра обеспечения кибербезопасности

В ходе реализации решения будут получены новые научные результаты:

- модель интеллектуальной распределенной системы управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечения процесса непрерывной идентификации;
- методика построения интеллектуальной распределенной системы управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечения процесса непрерывной идентификации;
- математическое и алгоритмическое обеспечение процессов функционирования интеллектуальной распределенной системы управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечения процесса непрерывной идентификации;
- универсальная интеллектуальная распределенная система управления кибербезопасностью на основе детерминированно-стохастических моделей и обеспечения процесса непрерывной идентификации (программный продукт), которая может быть внедрена в социальные и экономические процессы субъектов РФ, а также в учебный процесс при подготовке специалистов УГСН 10.00.00 «Информационная безопасность».

СПИСОК ЛИТЕРАТУРЫ

1. Котенко, И.В. Команды агентов в киберпространстве: моделирование процессов защиты информации в глобальном интернете / И.В. Котенко, А.В. Уланов // Труды Института системного анализа Российской академии наук – 2006 - Т. 27. - С. 108-129
2. Зегжда, Д.П. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации / Д.П. Зегжда, Ю.С.

Васильев, М.А. Полтавцева, И.Ф. Кефели, А.И. Боровков // Вопросы кибербезопасности – 2018 - № 2 (26) - С. 2-15

3. Путято, М.М. Адаптивная система комплексного обеспечения безопасности как элемент инфраструктуры ситуационного центра / М.М. Путято, А. С. Макарян, А.Н. Черкасов // Прикаспийский журнал: управление и высокие технологии. - 2020. - №. 4 (52). - С. 75-84.
4. Путято, М.М. Кибербезопасность как неотъемлемый атрибут многоуровневого защищенного киберпространства / М.М. Путято, А.С. Макарян // Прикаспийский журнал: управление и высокие технологии. - 2020. - №. 3 (51). - С. 94-102.

Магомедова Д.И.

Московский технический университет связи и информатики,

руководитель НОЦ ИБ ЛК,

d.i.magomedova@mtuci.ru

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДОВ И АЛГОРИТМОВ МАРКИРОВКИ НЕПОДВИЖНЫХ ИЗОБРАЖЕНИЙ И АУДИО СИГНАЛОВ С ИСПОЛЬЗОВАНИЕМ ФРАКТАЛЬНЫХ ПРОЦЕССОВ ДЛЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ.

Целью исследования является разработка методов и алгоритмов маркировки неподвижных изображений и аудио сигналов, устойчивых к воздействию атак, с использованием фрактальных процессов для защиты авторских прав.

Использование чужой интеллектуальной собственности в коммерческих целях является актуальной проблемой на сегодняшний день. Существует огромное количество удобных и доступных средств обработки медиа файлов, позволяющих вносить изменения и искажать оригинальные работы. Наиболее подвержены вмешательствам подобного рода неподвижные изображения и аудио файлы.

Стеганографические методы добавления ЦВЗ частично решают эту проблему. Вместе с тем у таких методов есть ряд недостатков, которые не позволяют использовать известные методы встраивания цифровых водяных знаков (ЦВЗ) для доказательства авторского права. К ним можно отнести низкую устойчивость к сжатию JPEG, частичное или полное удаление ЦВЗ при воздействии случайных и намеренных атак [1,2].

Проведенные исследования свидетельствуют о необходимости разработки новых методов добавления ЦВЗ в стегоконтейнеры, способные решать поставленные задачи.

Одним из методов решения поставленных задач является использование фрактального гауссовского шума для коррекции коэффициентов вейвлет разложения оригинального стегоконтейнера при встраивании ЦВЗ. В качестве ЦВЗ предлагается использовать псевдослучайную последовательность, характеризующую обладателя авторских прав. Такой подход к добавлению ЦВЗ является универсальным как для изображений, так и для аудио файлов [3].

Для количественной оценки качества разработанных методов встраивания ЦВЗ предлагаются следующие подходы:

1. Использование статистических метрик для оценки качества маркированных объектов после встраивания ЦВЗ.

2. Использование корреляционной функции для сравнения встроенного и извлеченного ЦВЗ.

3. Моделирование атак, направленных на удаление и искажение ЦВЗ, для оценки устойчивости разработанных алгоритмов.

4. Использование методов машинного обучения для оценки устойчивости разработанных алгоритмов к методам стегоанализа.

В рамках проекта предполагается проведение исследований по выбору типа и параметров вейвлет разложения с целью встраивания фрактального шума для обеспечения заданной достоверности извлечения ЦВЗ при высоком качестве воспроизведения оригинального стегоконтейнера.

Научный проект является частью диссертационной работы, которая направлена на исследование фрактальных методов маркировки изображений и аудио сигналов для защиты авторских прав.

В процессе диссертационной работы было произведено исследование использования различных алгебраических фракталов в целях оптимизации известных методов встраивания ЦВЗ в изображения. Анализировались известные методы встраивания ЦВЗ – метод замены наименее значащего бита (НЗБ) и метод замены коэффициентов дискретного косинусного преобразования (ДКП) [4].

Было предложено использовать алгебраические фракталы в виде промежуточных ключей и в виде ключей для определения области встраивания [5, 6]. Показано, что при добавлении ЦВЗ предложенными методами требуется знание параметров алгебраических фракталов на передающей и приемной стороне. Это заметно усложняет процесс несанкционированного доступа к добавленному ЦВЗ и не решает проблему устойчивости к сжатию и атакам.

Исходя из полученных результатов, была предложена комбинация методов стеганографии с использованием коэффициентов дискретного вейвлет-преобразования и алгебраических фракталов, что позволило повысить достоверность встраивания ЦВЗ при воздействии атак типа сжатия JPEG.

Другим нерешенным вопросом остается объективная оценка качества извлечения с использованием методов машинного обучения.

Предложенное направление научного проекта направлено на решение всех поставленных задач.

Результатом проекта станет создание алгоритма маркировки, который будет использоваться для защиты медиа контента от кражи и несанкционированного использования.

СПИСОК ЛИТЕРАТУРЫ

1. Шелухин О.И. Стеганография. Алгоритмы и программная реализация / Шелухин О.И., Канаев С.Д. – Горячая линия Телеком – М, 2018 – 592 с.
2. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Конахович Г.Ф., Пузыренко А.Ю. – МК-Пресс – Киев, 2006 – 285 с.
3. Sheluhin O. I. "Marking Audio Signals Using Fractal Gaussian Noise" / O. I. Sheluhin, D. I. Magomedova, S. Y. Rybakov and A. G. Simonyan //2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO) – 2021 - pp. 1-4
4. Bender W. Techniques for Data Hiding / Bender W., Gruhl D., Morimoto N., Lu A. // IBM Systems Journal – 1996 - № 35 - pp. 313-336.
5. Магомедова Д. И., Симонян А. Г., Смычѐк М. А. Использование алгебраических фракталов для защиты информации стеганографическими методами от несанкционированных воздействий // Вестник НГИЭИ. 2018. № 8 (87). С. 5–15.
6. Magomedova D.I. "Fractal Models and Algorithms for Creating a Protective Marking for Integrity and Authenticity Bitmap Images" / D. I. Magomedova, O. I. Sheluhin // 2020 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO) – 2020 - pp. 1-6.

Изергин Д.А.
Российский технологический университет – МИРЭА,
аспирант,
izergin@mirea.ru

МЕТОД ОБНАРУЖЕНИЯ КАНАЛОВ КОМПРОМЕТАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ НА МОБИЛЬНЫХ ОПЕРАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛИЗИРОВАННЫХ СРЕДСТВ ПРИНЯТИЯ РЕШЕНИЯ

Наиболее серьёзные угрозы сохранности конфиденциальных данных представляют приложения, предназначенные для сбора данных, перехвата событий взаимодействия пользователя с экраном или скрытого удалённого управления. Для детектирования вредоносных функций и недекларированных возможностей приложений используются различные методы сигнатурного и поведенческого анализа. Данные методы обладают рядом недостатков в условиях функционирования на мобильных устройствах. В мобильной разработке применение методов динамической загрузки исполняемого кода или обфускации является распространённым явлением, что существенно понижает эффективность сигнатурных методов анализа кода [1]. Также применение классического метода поиска утечек конфиденциальных данных taint — анализ (анализ помеченных данных) осложнено повсеместным использованием фреймворков «внедрения зависимости» (DI - Dependency injection) [2]. Данные фреймворки используют Reflection Api, что делает невозможным качественное построение графа потоков данных [3]. В свою очередь, проведение полноценного поведенческого анализа приложений является затруднительным в связи с ограниченными аппаратными ресурсами и предъявляемыми требованиями пользователей к быстродействию

устройства, что приводит к использованию облачной инфраструктуры, понижающей оперативность детектирования нарушения безопасности системы. Стоит отметить, что проведение поиска каналов утечки персональных данных в отдельных приложениях, установленных на мобильное устройство, не является полноценным средством защиты от создания цифрового портрета владельца устройства, т.к. не учитывает возможности объединения разрешений с целью получения доступа к ресурсам устройства. Таким образом, проведенный анализ существующих научных подходов и практических решений данной тематики [4-8] позволил выявить, что требуется решение ряда научно-технических задач, в частности:

– повышение точность связывания авторов сервисов;

– выявление подозрительных приложений на основе сформированного цифрового портрета;

– отсутствие методов автоматизированного связывания разработчиков сервисов на основе данных из открытых источников и исполняемых файлов;

– детектирование возможности агрегирования пользовательских данных из различных источников.

Анализ выделенных задач позволяет сформировать следующие противоречия:

1. В практике между потребностью в механизмах детектирования каналов сбора персональных данных различными сервисами на мобильных устройствах и требованиями пользователей к обеспечению защиты конфиденциальных данных.

2. В науке между потребностью в обеспечения заданной достоверности детектирования каналов сбора персональных данных и отсутствием научно-методического обоснования алгоритмов детектирования каналов сбора требуемым разрешением

В качестве путей решения противоречий возможно использовать:

– построение типичных цифровых портретов различных категорий приложений с целью выделения аномального поведения;

– разработка алгоритма выделения связующих признаков владельцев приложений;

– многомодельный подход к оцениванию рисков компрометации персональных данных на мобильных устройствах.

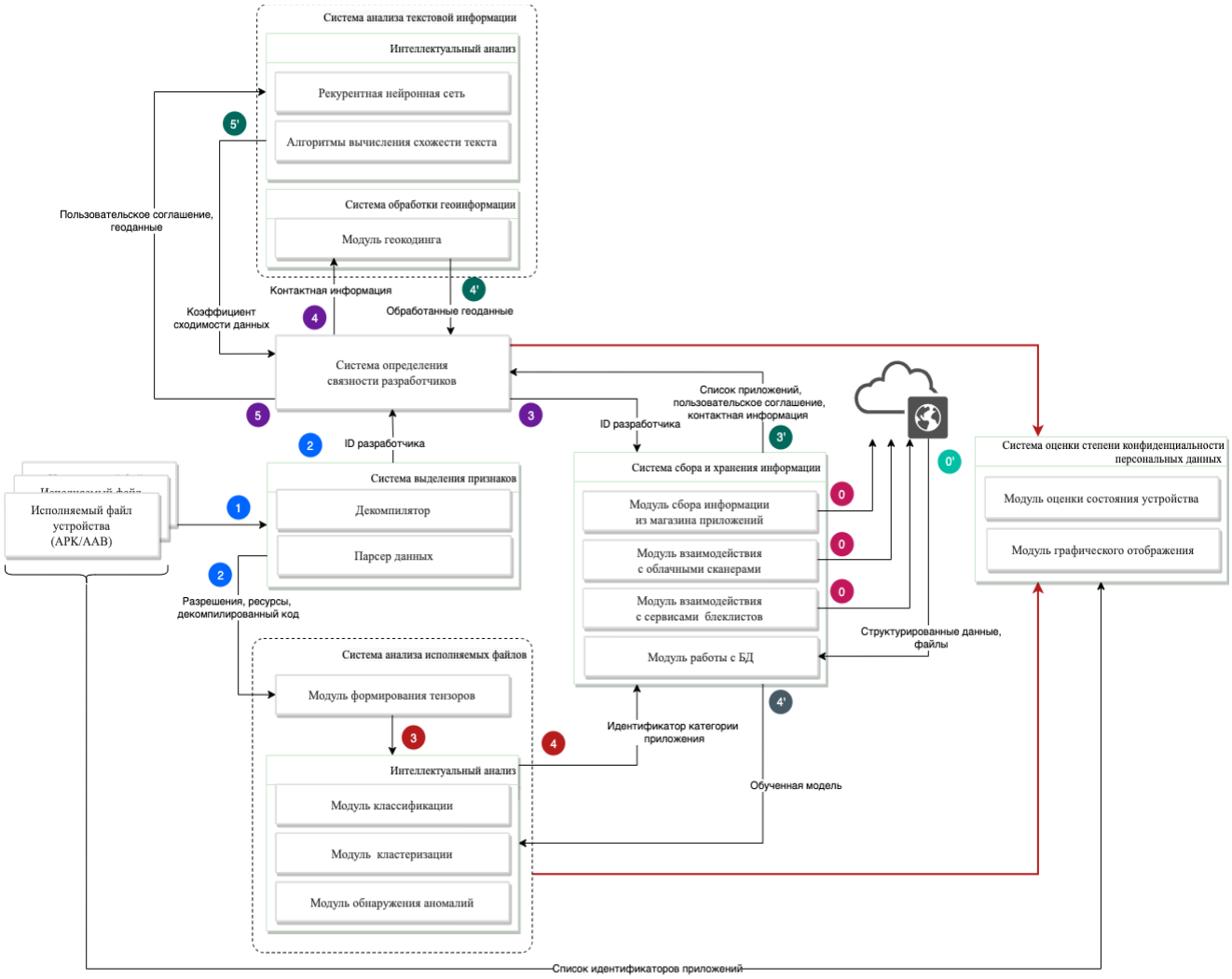

Рис. 1 Концептуальная схема функционирования системы обнаружения каналов утечки данных

На рис.1 представлена концептуальная схема функционирования системы обнаружения каналов утечки данных. Система состоит из четырёх основных подсистем: сбора информации из открытых источников и её хранения, анализа исполняемых файлов, анализа текстовой информации (входные данные: описание приложения, пользовательское соглашение, контактные данные) и оценки степени сохранности конфиденциальных данных.

В условиях, когда вопрос противодействия сбору и агрегированию информации из различных приложений является нерешённым, актуальность проводимой работы является высокой. Результат работы направлен на повышение уровня защиты персональных данных и обеспечения возможности отслеживания агрегирования информации различными источниками.

СПИСОК ЛИТЕРАТУРЫ

1. Фамилия 1-го автора, И.О. Nonlinear iterative precoding algorithm for MIMO multiuser systems / И.О. 1-я фамилия, И.О. 2-я фамилия // Название журнала. — Год выпуска. — № журнала. — Страницы.
2. Vikas Sihag. A survey of android application and malware hardening / Vikas Sihag, Manu Vardhan, Pradeep Singh // Computer Science Review. — 2021. — 39. – 100365.
3. Linghui Luo. A Qualitative Analysis of Android Taint-Analysis Results / Linghui Luo; Eric Bodden; Johannes Spath // 34th IEEE/ACM International Conference on Automated Software Engineering (ASE). — 2019. — 102-114.
4. Zhuo Ma. A Combination Method for Android Malware Detection Based on Control Flow Graphs and Machine Learning Algorithms / Zhuo Ma, Haoran Ge, Yang Liu // IEEE Access PP. — 2019. — 99. — 1–11.

5. Nattanon Wongwiwatchai. Detecting personally identifiable information transmission in android applications using light-weight static analysis / Nattanon Wongwiwatchai, Phannawhat Pongkham, Kunwadee Sripanidkulchai // Computers&Security. — 2020. — 99(4). — 102011.
6. Jinhong YANG. Aggregated Risk Modelling of Personal Data Privacy in Internet of Things / Jinhong YANG, Chul-Soo KIM, Md Mehedi Hassan ONIK // 21st International Conference on Advanced Communication Technology (ICACT). — 2019. — 425–430.
7. Md Mehedi Hassan Onik. Personal Information Classification on Aggregated Android Application's Permissions / Md Mehedi Hassan Onik, Chul-Soo Kim, Nam-Yong Lee, Jinhong Yang // Applied Sciences. — 2019. — 9. — 3997.
8. Anastasia Shuba. On-Device Detection of Personal Information Exposure / Anastasia Shuba, Evita Bakopoulou, Milad Asgari Mehrabadi, Hieu Le, David Choffnes2, Athina Markopoulou // arXiv:1803 [cs.NI]. — 2018. — 01261.

Баранов В. В.

Южно-Российский государственный политехнический университет имени М.И. Платова, заведующий кафедрой «Информационная безопасность», кандидат военных наук, доцент,

baranov.vv.2015@yandex.ru

МЕТОДИЧЕСКИЕ ОСНОВЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ РАЗРАБОТКЕ СИСТЕМ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Наиболее сложным аспектом в процессе разработки систем защиты является полнота и качество оценки угроз безопасности информации, принятие обоснованного решения об их актуальности, а также выбор комплекса мер и средств защиты информации, эффективных в складывающейся обстановке.

На этапе функционирования, в условиях динамично меняющегося деструктивного воздействия, система защиты требует непрерывного оперативного управления, своевременного и обоснованного реагирования на возникающие новые риски и угрозы безопасности информации (УБИ).

Реализация данной задачи может быть осуществлена путем разработки комплексной динамической модели безопасности защищенных информационных систем различного назначения в условиях деструктивного воздействия (ДВ), позволяющей также моделировать процесс оперативного управления событиями ИБ в условиях изменений воздействующих факторов.

Основу данной модели составляют типовые модули (Рис.1).

В составе типового модуля выделены четыре зоны (кластера):

1. Зона моделирования рисков угроз безопасности информации.

2. Зона моделирования способов ликвидации рисков угрозы инцидента.

3. Зона моделирования рисков инцидента.

4. Зона моделирования способов ликвидации последствий инцидента.

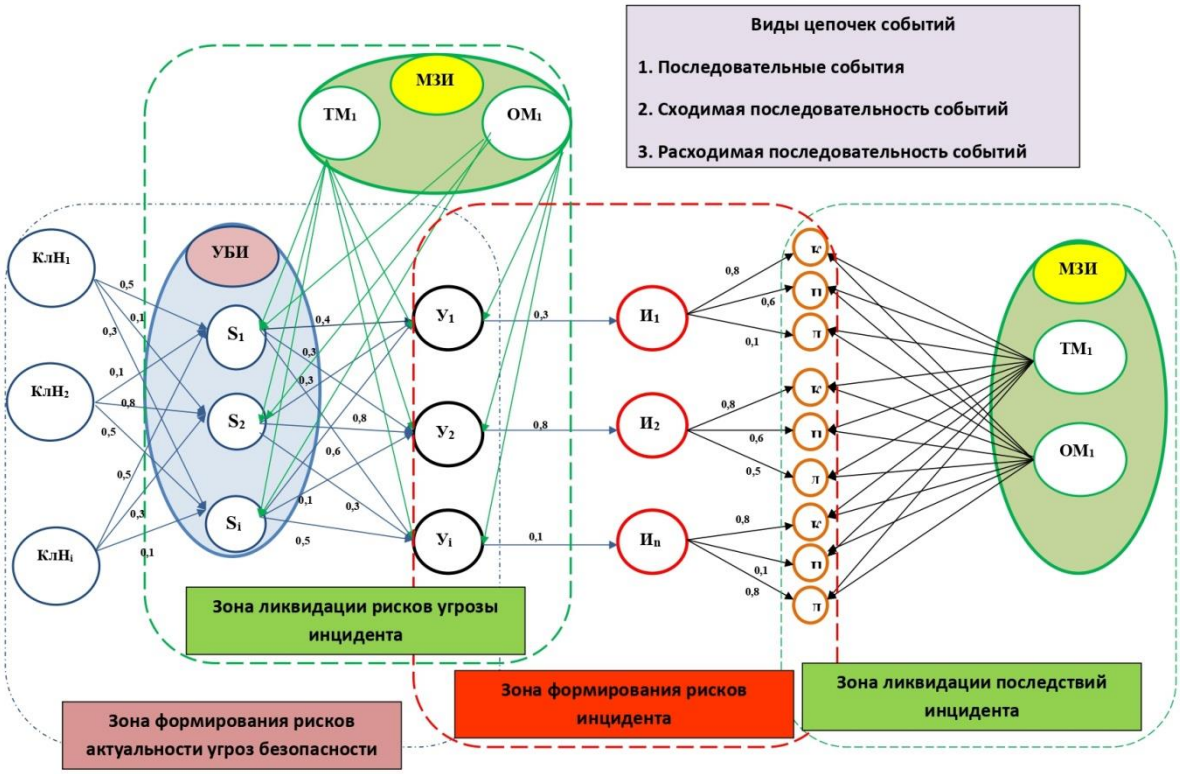

Рис. 1. Типовой модуль комплексной динамической модели безопасности защищенных информационных систем

В основе данной модели положена байесовская сеть [1, 2]. Она представлена как совместное распределение вероятностей с использованием направленного ациклического графа, в котором каждое ребро является условной зависимостью показателей ДВ и показателей мер защиты информации (МЗИ), а каждый узел представлен отдельной случайной величиной, отражающей события ИБ.

В модели взаимное влияние деструктивных воздействий и способов реализации МЗИ можно выделить в виде цепочек последовательных событий, а также сходимой и расходимой последовательностей событий.

Вычисление для указанных видов последовательностей событий осуществляется по указанным ниже формулам.

Последовательные события (1):

$$P(K_{Л}H_i, У_i \mid S_i) = P(Кл\ H_i \mid S_i) \cdot P(У_i \mid S_i) \quad (1)$$

Сходимая последовательность событий (2):

$$P(TM_i, OM_i, У_i) = \sum_{У_i} P(TM_i)P(OM_i)P(У_i \mid OM_i, TM_i) = P(OM_i)P(TM_i) \quad (2)$$

Расходимая последовательность событий (3):

$$P(TM_i, OM_i, У_i) = \sum_{У_i} P(TM_i)P(OM_i)P(У_i \mid OM_i, TM_i) = P(OM_i)P(TM_i) \quad (3)$$

Такой подход позволяет реализовать процесс вычисления апостериорного распределения переменных риска реализации инцидентов по переменным показателей деструктивного воздействия и переменным показателей МЗИ, который называют вероятностным выводом. Для его проведения в работе используются алгоритмы кластеризации. В виде кластеров представлены указанные выше зоны моделирования [3].

Исходные данные для моделирования событий ИБ в динамике складывающейся ситуации получаем с сайтов ФСТЭК, ФСБ, международных баз данных и из специфических данных, характерных для объекта.

Данная методика даёт возможность проведения универсальной оценки для событий информационной безопасности по количественным значениям подмножества переменных показателей МЗИ и деструктивного воздействия нарушителей, который минимизирует вероятность ошибочного решения [4, 5].

При принятии решения зачастую важна качественная оценка событий ИБ. Для перевода количественной оценки риска реализации инцидента ИБ в качественную, применим следующий нечетко-вероятностный метод [6].

1. Зададим совместное распределение вероятностей событий ИБ $\{P(КлН_i,S_i,У_i)|P(ТМ_i,ОМ_i,)\}$., где $P(ТМ_i,ОМ_i,)$ вероятная эффективность способа реализации МЗИ, $P(КлН_i,S_i,У_i)$ – вероятность риска реализации УБИ.

2. Проведем преобразование нечетких значений входных переменных {P(КлНi,Si,Уi) и P(ТМi,ОМi,)} «Очень низкий (ОН)», «Низкий (Н)», «Средний (С)», «Высокий (В)», «Очень высокий (ОВ)» в числовые значения [7].

3. Зададим формулы оценки и преобразование нечетких значений оценки риска реализации инцидента ИБ в числовые значения из диапазона [0, 1], матрицы нечетких правил оценки риска реализации инцидента ИБ (Рис.2).

		Вероятная эффективность способа реализации МЗИ				
		ОН	**Н**	**С**	**В**	**ОВ**
Вероятность риска реализации УБИ	**ОН**	Н	Н	С	В	ОВ
	Н	Н	Н	С	В	ОВ
	С	Н	Н	С	В	ОВ
	В	Н	Н	С	В	ОВ
	ОВ	Н	Н	С	В	ОВ

Рис. 2. Матрица нечетких правил оценки риска реализации инцидента

4. Осуществим перевод оценки из количественной в качественную (Табл.1).

Табл. 1. Соотношение оценок риска реализации инцидента ИБ

Значения количественной оценки риска реализации инцидента	**Значения качественной оценки риска реализации инцидента**
$0 \le P(S_i V_i \mid И_i) \le 0,2$	Очень низкая
$0,2 \le P(S_i V_i \mid И_i) \le 0,4$	Низкая
$0,4 \le P(S_i V_i \mid И_i) \le 0,6$	Средняя
$0,6 \le P(S_i V_i \mid И_i) \le 0,8$	Высокая
$0,8 \le P(S_i V_i \mid И_i) \le 1$	Очень высокая

Разработанная модель масштабируема, а значит, обладает свойствами универсальности как по критериальным требованиям, так и вероятностным показателям. На ее базе возможно осуществить нейробаесовсий подход и получить систему поддержки принятия решений на основе искусственного интеллекта [8].

СПИСОК ЛИТЕРАТУРЫ

1. Перл Д. Байесовские сети/ Д. Перл — М.: UCLA Cognitive Systems Laboratory, 2000. - 102 с.
2. Джексен Ф. Байесовские сети и графы решений / Ф. Джексен. — М.: Sprinnger, 2001. - 220 с.
3. Скворцов Ю.С., Подходы к построению систем поддержки принятия решений на основе байесовских сетей / Скворцов Ю.С., Сапронов В. А. // Интеллектуальные информационные системы: Труды всероссийской конференции. – Воронеж, 2016. – 41-43 с.
4. Норвиг П. Искусственный интелект: современный подход / П. Норвиг. — М.: Вильямс, 2007. - 1408 с.

5. Кудашев О.Ю. Проблемы инициализации систем сегментации дикторов на основе вариационного байесовского анализа / Кудашев О.Ю., Пеховский Т.С., // «Компьютерные и информационные науки». – 2019. №79. – С.79-84.
6. Гавришев, А.А. Анализ программ моделирования нечетких систем / А.А. Гавришев, А.П. Жук // Дистанционное и виртуальное обучение. – 2017. – № 6. – С. 76-83.
7. Гавришев, А.А. Моделирование и количественно-качественный анализ распространенных защищенных систем связи / А.А. Гавришев // Прикладная информатика. – 2018. – Т. 13. – № 5 (77). – С. 84-122.
8. Воронцов К.В. Модификации EM-алгоритма для вероятностного тематического моделирования / Воронцов К.В., Потапенко А.А.,// «Машинное обучение и анализ данных». – 2016. №284. – С.657-667.

Буртыка Ф.Б.
Южный федеральный университет,
младший научный сотрудник,
bbfilipp@yandex.ru

О ПРЕОБРАЗОВАНИЯХ ПРОГРАММ ДЛЯ ПРОВЕДЕНИЯ ВЫЧИСЛЕНИЙ НАД ЗАШИФРОВАННЫМИ ДАННЫМИ

Гомоморфное шифрование (ГШ) — вид шифрования, позволяющий проводить определённые математические операции над зашифрованными данными и получать зашифрованный результат, который соответствует результату операций, выполненных над незашифрованными данными. ГШ имеет несколько разновидностей, включая полностью гомоморфное шифрование (ПГШ) и вполне гомоморфное шифрование (ВГШ).

Часто называемое «Святым Граалем» криптографии, ПГШ позволяет выполнять *любые произвольные* вычисления для зашифрованных данных, выраженные через операции сложения и умножения [1].

ВГШ [1] также позволяет выполнять как сложение, так и умножение, но только *ограниченного количества* операций, после которых шифртекст теряет целостность и больше не может быть правильно расшифрован.

Большинство современных схем ГШ основаны на задаче «Learning with Errors» (LWE) [1], и предполагает добавление шума к шифртекстам. Пока шум достаточно мал, шифртекст можно расшифровать в правильное сообщение. Во время гомоморфных операций шум в шифротексте растет. В то время как этот эффект незначителен во время сложения, умножение двух шифротекстов значительно увеличивает общее количество шума. В результате только фиксированное количество последовательных умножений (параметр, называемый мультипликативной глубиной) может быть выполнено до того,

как расшифрование станет невозможным. Это ограничение можно обойти с помощью «самокоррекции» — метода, который сбрасывает уровень шума шифротекста на более низкий уровень путем гомоморфного вычисления схемы расшифрования (то есть алгоритма, который преобразует шифртекст в открытый текст) с зашифрованным секретным ключом в качестве входных данных.

Разработка программного обеспечения, использующего ГШ, представляет собой уникальную проблему при выборе параметров. Для конкретного вычисления необходимо выбрать правильный набор параметров, который позволяет избежать самокоррекции, при этом обеспечивает криптостойкость и гарантирует, что размер шифротекста остается управляемым. Это также включает выбор правильной схемы кодирования для правильных вычислений. Например, двоичное кодирование предпочтительнее для логических операций (например, TFHE [2]), а арифметическое кодирование предпочтительнее для арифметических вычислений (например, BGV[3] и BFV [4]).

ГШ приближается к тому, чтобы стать практичным, но все еще требует значительного опыта, чтобы использовать его в разработке программного обеспечения. Помимо понимания необходимых криптографических параметров, предыдущая работа в основном была сосредоточена на поддержке низкоуровневых примитивов программирования (например, арифметических операторов или булевой логики), поэтому разработчикам необходимы дополнительные знания в области низкоуровневого проектирования программного обеспечения, чтобы использовать эти примитивы и создавать более сложные программы. При разработке приложений ГШ в настоящее время *отсутствует* инструментарий для разработчиков, не обладающих знаниями в области криптографии, для написания кода без понимания

криптосистемы, лежащей в основе. Транспилятор ГШ может восполнить этот пробел.

Транспилятор [5] - это инструмент, который преобразует один исходный текст программы на языке высокого уровня в другой исходный текст этой же программы на языке высокого уровня. Транспилятор ГШ получает код, написанный на языке высокого уровня (например, C++ или Pascal), и создает эквивалентный код, способный обрабатывать зашифрованные входные данные.

Как недавно упоминали Виандand соавторы [6], недостающий компонент для использования ГШ представляет собой серию чистых уровней абстракции, которые отделяют бизнес-логику (то есть то, чего пытается достичь разработчик) от промежуточного представления (то есть того, как системы нижнего уровня могут оперировать или оптимизировать это) и оптимизированной низкоуровневой реализации (то есть, какие библиотеки и системы элементарных машинных команд могут использоваться для поддержки этих первых двух уровней). В идеале, самый верхний уровень должен принимать в качестве входных данных высокоуровневые языки [7], позволяя промежуточным уровням оставаться достаточно выразительными для представления элементарных логических и арифметических операций, чтобы воспользоваться преимуществами различных схем ГШ и, при необходимости, выполнять трансляцию между ними [8].

Одной из наиболее актуальных на сегодняшний день проблем является преобразовать приложение в соответствующее схемное вычисление. Например, разрабатываемые инструменты могли бы автоматически векторизовать итеративно написанные программы или предлагать подсказки по некоторым аспектам вычислений, в стиле диалоговых распараллеливающих систем [9]. В целом, аппарат распараллеливающих преобразований программ хорошо подходит для создания инструментов

преобразований программ к виду, допускающему гомоморфные вычисления, поскольку основные задачи в обоих случаях очень похожи: устранение зависимостей по данным, векторизация циклов и т.д.

СПИСОК ЛИТЕРАТУРЫ

1. Бабенко, Л.К. Полностью гомоморфное шифрование (Обзор) / Л.К. Бабенко, Ф.Б. Буртыка, О.Б. Макаревич, А.В. Трепачева // Вопросы защиты информации. — 2015. — № 3. — С. 3-26.
2. Chilotti, I. TFHE: Fast Fully Homomorphic Encryption over the Torus / I. Chilotti, N. Gama, M. Georgieva, M. Izabachene // Journal of Cryptology. — 2020. — № 1. — Стр. 34-91.
3. Brakerski, Z. (Leveled) Fully Homomorphic Encryption without Bootstrapping. / Z. Brakerski, G. Craig, V. 2-я фамилия // ACM Transactions on Computation Theory. — 2014. — № 3. — Стр. 1-36.
4. Fan, J. Somewhat Practical Fully Homomorphic Encryption / J. Fan, F. Vercauteren // Cryptology ePrint Archive, Report 2012/144. — 2012. — № 144. — https://eprint.iacr.org/2012/144.
5. Gorantala, S. A General Purpose Transpiler for Fully Homomorphic Encryption / S. Gorantala и др. // arXiv preprint arXiv:2106.07893. — 2021.
6. Viand, A. SoK: Fully Homomorphic Encryption Compilers / A. Viand, P. Jattke, A. Hithnawi // Proceedings of Symposium on Security and Privacy. IEEE. — 2021.
7. Бабенко, Л.К. Обобщенная модель системы криптографически защищенных вычислений / Л.К. Бабенко, Ф.Б. Буртыка, О.Б. Макаревич, А.В. Трепачева // Известия ЮФУ. Технические науки. — 2015. — № 5. — С. 77-86.

8. Boura, C. CHIMERA: Combining Ring-LWE-based Fully Homomorphic Encryption Schemes / C. Boura, N. Gama, M. Georgieva, D. Jetchev // Journal of Mathematical Cryptology. — 2020. — № 1, Vol. 14. — С. 316-338.
9. Штейнберг, Б.Я. Особенности реализации распараллеливающих преобразований программ в системе ДВОР / Б.Я. Штейнберг и др. // Известия высших учебных заведений. Приборостроение. — 2011. — № 10. — С. 87-89.

Сергеев А.В.

Московский институт электроники и математики

НИУ «Высшая школа экономики», советник,

avsergeev@hse.ru

ОЦЕНКА ВЫИГРЫША ПРИ ИСПОЛЬЗОВАНИИ СТАТИСТИЧЕСКОЙ МОДУЛЯЦИИ НА ПРИМЕРЕ QAM16 ДЛЯ ЭКСПОНЕНЦИАЛЬНО РАСПРЕДЕЛЕННЫХ ВХОДНЫХ ДАННЫХ

Большинство современных систем передачи данных исходят из предположения, что распределение символов данных, поступающих на вход блока модуляции, близко к равномерному распределению. Это предположение основывается, обычно, на том факте, что перед кодированием и модуляцией, передаваемые данные подвергаются пред-обработке (сжатию, шифрованию и т.п.) приводящим к «выравниванию» вероятностей символов информационного потока.

Основное вопрос работы – как изменится эффективность модуляции, если (а) предположить, что поступающие символы имеют распределение отличное от равномерного и (б) если модуляционная схема учитывает этот факт. В качестве системы модуляции выбрана квадратурно-амплитудная модуляция (рус. КАМ, англ. QAM) в силу её широкого применения на практике.

Важным параметром, который необходимо оценить при этом, является средняя энергия сигнала после модуляции. Ниже этот параметр оценивается для КАМ при равномерном и экспоненциальном распределении входных символов.

В качестве базового примера рассмотрим сравним варианты, когда входной поток символов, поступающих на модуляционную схему, имеет

равномерное («классический» QAM) и экспоненциальное распределение (СКАМ).

Основная идея статистического КАМ (СКАМ) для экспоненциального распределения состоит в том, чтобы отображать наиболее частые входные символы в точке на созвездии КАМ с наименьшей энергией передачи. В результате средняя энергия системы передачи значительно снижается, поскольку значения символов после модуляции с низкой энергией передаются более часто, чем значения с более высоким уровнем энергии. В литературе такой подход также имеет название «constellation shaping» (рус. «шейпинг созвездия»).

На практике подобный поток символов встречается очень часто: передача несжатого текста, разностного видео потока, команд управления и т.п.

Графическая интерпретация распределения точек сигнального созвездия на приемной стороне (после передачи через AWGN-канал) показана на рис. 1.

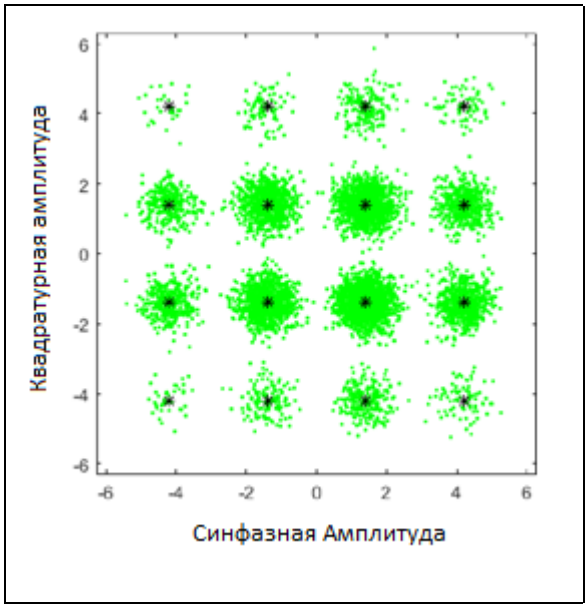

Рис. 1. Экспоненциальное распределение в статистической КАМ с наложенным шумом

Для корректности сравнения двух модуляционных схем (СКАМ и КАМ) необходимо выровнять среднюю энергию передачи. Средняя энергия СКАМ может быть увеличена за счет увеличения расстояния между точками в созвездии.

Для корректности сравнения двух модуляционных схем (СКАМ и КАМ) необходимо выровнять среднюю энергию передачи. Средняя энергия СКАМ может быть увеличена за счет увеличения расстояния между точками в созвездии.

Результаты итогового сравнения КАМ/СКАМ для критерия BER/SNR показаны на рисунке 4. Программная модель передачи с использованием КАМ16/СКАМ реализована на MatLab. Для моделирования канала используется простая модель с аддитивным белым гауссовским шумом. После переддачи производится демодуляция на приемнике, после этого подсчитывается количество ошибочных бит, строится кривая зависимости ошибок на бит от отношения сигнала к шуму. Результаты. Графики зависимостей ошибки на бит и отношения сигнал-шум, полученные в результате моделирования, хорошо согласуются с теоретическими формулами.

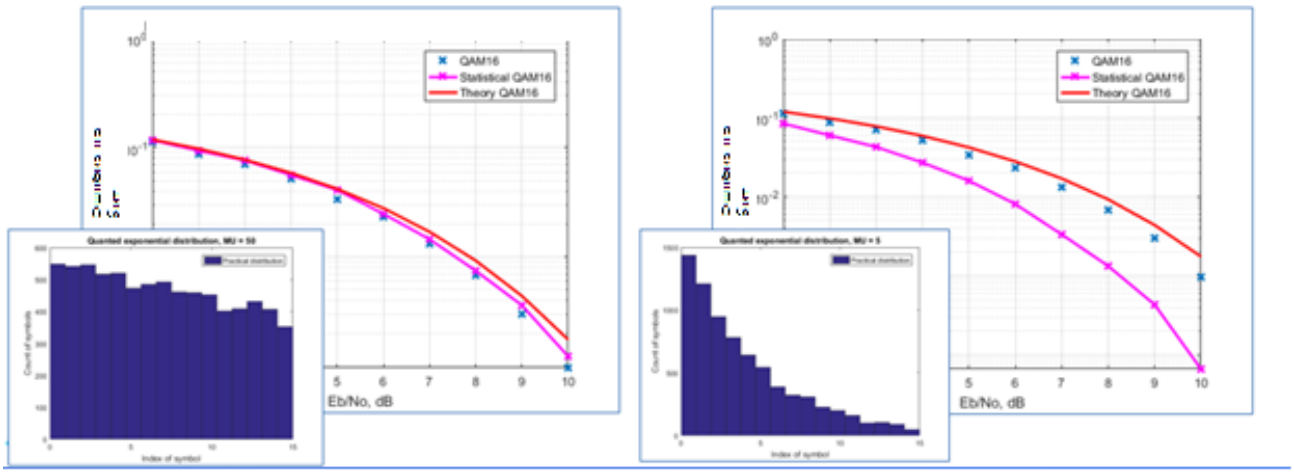

Рис. 2. Сравнение QAM/SQAM для критерия BER/SNR

СПИСОК ЛИТЕРАТУРЫ

1. A.V. Sergeev, The Evaluation of Gain of Statistical Modulation Method on the Example of QAM16 for Input Data with Exponential Distribution / A. V. Sergeev ; R. R. Shanyazov ; D. V. Ilina ; V. V. Bashun // Proc. Of Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), 2018

Трепачева А.В.
Южный федеральный университет,
младший научный сотрудник,
alina1989malina@yandex.ru

О ПОДХОДАХ К ОЦЕНКЕ КРИПТОСТОЙКОСТИ АЛГЕБРАИЧЕСКИ ГОМОМОРФНЫХ ШИФРОВ, ОСНОВАННЫХ НА ЗАДАЧЕ ФАКТОРИЗАЦИИ ЧИСЕЛ

Гомоморфное шифрование — вид шифрования, позволяющий проводить определённые математические операции над зашифрованными данными и получать зашифрованный результат, который соответствует результату операций, выполненных над незашифрованными данными. Эффективное и криптостойкое гомоморфное шифрование дает принципиально новые возможности по обеспечению информационной безопасности в таких областях как облачные вычисления, медицинские и финансовые данные, и т. д., поскольку позволяет проводить обработку зашифрованных данных в недоверенной среде без их расшифрования.

Предложено уже довольно большое количество алгебраически гомоморфных криптосистем, стойкость которых авторы предполагается авторами сводящейся к задаче факторизации чисел (эта задача считается эталоном сложной задачи в компьютерной безопасности), однако подробного анализа криптостойкости проведено не было.

Вообще говоря, в настоящее время в литературе есть несколько методов криптоанализа алгебраически гомоморфных шифров, основанных на задаче факторизации чисел: это, прежде всего, метод вычисления результанта [1], метод нахождения наибольшего общего множителя [2,3] и метод линейных преобразований [4].

Одним из инструментов для обобщенного теоретического криптоанализа гомоморфных криптосистем, основанных на факторизации чисел в настоящее время являются т. н. закрытые кольца (black-box ring) [5, 6, 7].

Определение 1 (black-box ring representation [5]). Пусть $(R, +, \cdot)$ – конечное кольцо, S – конечное множество битовых строк, такое что $|S|=|R|$. Набор (σ, O), состоящий из случайно выбранной кодирующей (биективной) функции $\sigma: R \to S$ и соответствующего оракула O закрытого кольца (вычисляющего по паре элементов их сумму или произведение), называется *закрытым представлением кольца* для R и обозначается R^σ.

Определение 2 (задача РЗК [5]). Пусть R – явно заданное конечное коммутативное кольцо с единицей 1 и известной характеристикой n. Кроме того, пусть $B := \{r_1,...,r_t\}$ – (явно заданное) порождающее множество R. Задача *распознавания в закрытом кольце* (РЗК) для R – это задача нахождения $x \in R$, где x выбирается из R случайно по равномерному распределению при заданном $\sigma(x), \sigma(1), \sigma_1,...,\sigma_t \in R^\sigma$.

Теорема 1 ([5]). Пусть $R := \mathbb{Z}_n$ для некоторого целого n, имеющего не менее двух различных простых множителей. Пусть A – алгоритм решения задачи РЗК, который выполняет не более $m \le n$ операций над R^σ. Предположим, что A решает задачу РЗК с вероятностью ε. Тогда существует алгоритм B, имеющий доступ к реализации A, который находит множитель n с вероятностью не менее

$$\frac{\varepsilon - \frac{1}{n}}{m^2 + 3m + 2},$$

запустив A один раз и выполнив дополнительное количество $O(m^2)$ случайных выборов и $O(m^3)$ операций кольца R, а также $O(m^2)$ вычислений наибольшего общего делителя на $\log_2 n$ -битных числах.

Таким образом, в [5] устанавливается, что сложность взлома гомоморфной над кольцом криптосистемы в общем случае равна сложности задачи факторизации чисел. Однако на практике мы видим [3, 8] что стойкость криптосистем, основанных на полиномиальных гомоморфизмах, фактически очень низкая. В чем же дело?

Если проанализировать примеры из [3, 8], то можно увидеть, что авторы криптосистем организуют зашифрование в два этапа, на первом из которых осуществляется вложение элемента кольца открытых текстов в кольцо, изоморфное кольцу шифртекстов, а на втором этапе используют в качестве биективных гомоморфизмов линейные замены переменных, количество которых в кольце $\mathbb{Z}[x_1,...,x_t]$ равно $n \cdot t$ где t – количество образующих. Однако, общее количество биекций, которые рассматриваются в модели закрытого кольца гораздо больше и равно $|R|!$, т.е числу всех перестановок элементов R (в случае $\mathbb{Z}[x_1,...,x_t]$ это $n^t!$).

В модели закрытого кольца не учитывается алгоритмическая сложность функции σ а также алгоритмов оракула O, с помощью которых производят операции кольца над закрытым представлением его элементов.

Предлагаемая в данной работе модель гомоморфной криптосистемы учитывает, что алгоритмическая сложность функции σ а также алгоритмов оракула O должна быть полиномиальна от $t \cdot \log n$. В этой модели легко показать, что взлом скрытого гомоморфизма не требует знания факторизации n и может быть выполнен в общем случае (основная идея состоит в том, что при зашифровании не может быть использована произвольная биекция, поскольку длина записи номера биекции не позволяет машине Тьюринга, представляющей σ, считать этот номер за полиномиальное время).

СПИСОК ЛИТЕРАТУРЫ

1. Brickell, E.F. On privacy homomorphisms / E.F. Brickell, Y. Yacobi // Advances in Cryptology—EUROCRYPT’87. — 1988. — С. 117-125.
2. Трепачева, А.В. О соотношениях между атаками на симметричные шифры, гомоморфные над кольцом вычетов / А.В. Трепачева // Безопасность информационных технологий. — 2017. — № 2. — Стр. 82-91.
3. Trepacheva, A. Cryptanalysis of Polynomial based Homomorphic Encryption / A. Trepacheva // Proceedings of the 7th International Conference on Security of Information and Networks. — 2014. — Стр. 205-210.
4. Vizar, D. Cryptoanalysis of Chosen Symmetric Homomorphic Schemes / D. Vizar, S. Vaudenay // Studia Scientiarum Mathematicarum Hungarica. — 2015. — № 2. — Стр. 288-306.
5. Altmann, K. On black-box ring extraction and integer factorization / K. Altmann, T. Jager, A. Rupp // Proceedings of the 35th international colloquium on Automata, Languages and Programming, Part II. — 2008. — С. 437-448.
6. Jager, T. On the analysis of cryptographic assumptions in the generic ring model / T. Jager, J. Schwenk // Journal of cryptology. — 2013. — № 2. — С. 225-245.
7. Borovik, A. Homomorphic encryption and some black box attacks / A. Borovik, Ş. Yalçınkaya // Proceedings of International Congress on Mathematical Software. — 2020. — С. 115-124.
8. Трепачева, А.В. Криптоанализ шифров, основанных на гомоморфизмах полиномиальных колец / А.В. Трепачева // Известия ЮФУ. Технические науки. — 2014. — № 8. — С. 96-107.