ISSN 2074-7128 (print), ISSN 2074-7136 (on-line)

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
(IT Security)

Периодический рецензируемый научный журнал «Безопасность информационных технологий», освещающий широкий спектр проблем обеспечения информационной безопасности, в том числе технологические, организационно-правовые и образовательные аспекты.

Журнал зарегистрирован в Государственном комитете Российской Федерации по печати.
Свидетельство № 017789.
Издается с 1994 г.

С момента основания и до настоящего времени учредителем журнала является федеральное государственное автономное образовательное учреждение высшего образования Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ).

С 2007 г. и по настоящее время журнал входит в Перечень ВАК ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук по отраслям науки и группе специальностей научных работников
05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей (технические науки),
05.13.19 – Методы и системы защиты информации, информационная безопасность (технические науки), по которым журнал входит в этот перечень.

Основные тематические направления журнала:

- *Концептуальные основы обеспечения информационной безопасности автоматизированных систем;*
- *Методические подходы к анализу и оценке рисков информационной безопасности, технологии поиска уязвимостей в программном обеспечении;*
- *Оценка уровня защищенности автоматизированных систем;*
- *Программно-технические способы и средства обеспечения информационной безопасности.*

Журналом приветствуются статьи на русском и английском языках.

IT Security (Russia)

IT Security is a periodic peer-reviewed scientific journal publishing papers on a wide range of information security topics, including technological, organizational, legal and educational problems.

Since its establishment in 1994 (registration certificate No. 017789 by the State Committee for Press of the Russian Federation), the journal has been publishing by the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University, a.k.a. "MEPhI" (Moscow Engineering Physics Institute).

Papers in Russian and English are equally welcome.

Focus topics:

- *Fundamentals of information security of automated systems;*
- *Methodology of assessing the information security risks;*
- *Technology of detecting software vulnerabilities;*
- *Evaluation of the security level of automated systems;*
- *Soft- and hardware means of ensuring information security.*

СОДЕРЖАНИЕ

CONTENT

ОТ ГЛАВНОГО РЕДАКТОРА

ОБРАЩЕНИЕ ГЛАВНОГО РЕДАКТОРА К АВТОРАМ И ЧИТАТЕЛЯМ

Editor in Chef Letter to the Authors and Readers

DOI: http://dx.doi.org/10.26583/bit.2022.1.01

Уважаемые коллеги!

Приступив к исполнению обязанностей главного редактора журнала «Безопасность информационных технологий», хочу поделиться с нашими авторами и читателями мыслями и планами по развитию и расширению проблематики издания. Конечно, все привычные для журнала научно-технические и методические вопросы развития системы информационной безопасности, защиты информации и соответствующих технологий, программных и аппаратных средств по-прежнему актуальны и остаются в центре нашего внимания. Вместе с тем, считаю полезным расширить тематику журнала и включить в нее актуальное и перспективное направление развития доверенных систем и радиоэлектронной аппаратуры (РЭА), а также электронной компонентной базы (ЭКБ) для их реализации, включая вопросы задания технических требований, методов и технологий обеспечения и контроля доверенности на всех этапах жизненного цикла изделий – в процессе их разработки, изготовления и эксплуатации в реальных условиях (в том числе при дестабилизирующих воздействиях).

Свойства и понятия доверенности принято относить к информации и средствам ее обработки, но эта категория пока еще не вполне устоялась применительно к доверенным ЭКБ и РЭА, доверенным процессам и технологиям их проектирования (Security by Design) и производства (Security by Process), а также подходам к верификации, тестированию и испытаниям изделий. Важно подчеркнуть, что категорию доверенности ЭКБ и РЭА следует рассматривать в широком смысле относительно всего спектра дестабилизирующих воздействий и угроз как искусственного, так и естественного происхождения. Это далеко выходит за рамки комплектования и обеспечения средств защиты информации (СЗИ), вооружения, военной и специальной техники (ВВСТ), которые составляют относительно небольшой объем от общей потребности в ЭКБ и РЭА, и по сути являются лишь видимой вершиной огромного «электронного айсберга»! Категория доверенности должна охватывать и объективно распространяться практически на всю инфраструктуру и аспекты нашей жизнедеятельности – промышленность, энергетику, торговлю и услуги, навигацию и связь, коммуникацию и транспорт (в т.ч. беспилотный), интернет вещей, коммунальное хозяйство, медицинские и диагностические системы, бытовую технику, системы видеонаблюдения и контроля доступа – перечень практически не ограничен. Даже современные кабели зарядки телефонов и автоматы защиты бытовой электросети в каждой квартире в своем составе содержат электронные компоненты, управляющие их работой и влияющие на доверенность. Таким образом, сегодня все – как традиционные, так и новые сферы нашей жизни – насыщены интеллектуальной электроникой и критически уязвимы для сбоев, отказов и несанкционированного вмешательства.

ЭКБ (РЭА) могут считаться доверенными если они:

– соответствуют требованиям нормативных документов и декларированным свойствам, характеристикам и параметрам в течение заданных сроков, в режимах и условиях эксплуатации у потребителя;

– не имеют недекларированных элементов, возможностей и каналов управления функционированием, считывания и искажения внутренней информации, нарушения работоспособности и других скрытых уязвимостей или каналов утечки информации;

– не имеют признаков контрафактной продукции и недокументированных изменений (коррекций), внесенных в процессе ее разработки и/или производства, и потенциально оказывающих влияние на их способность удовлетворять потребности в соответствии с назначением.

Таким образом, категория доверенности ЭКБ (РЭА) включает в себя совокупность следующих неотъемлемых свойств изделия, которые требуют нормирования и подтверждения:

– качество, как свойство изделия удовлетворять потребности в соответствие с назначением и описанием;

– надежность, как способность сохранять качество в течение всего периода эксплуатации;

– живучесть и стойкость, как способность сохранять качество в реальных условиях эксплуатации;

– верифицированность и тестопригодность (адаптированность для повторной верификации в независимой лаборатории), как гарантированное и документально подтвержденное соответствие декларированным составу и техническим свойствам, параметрам, функциональным и эксплуатационным характеристикам;

– обеспечение безопасности информации, как результат испытаний на отсутствие недекларируемых элементов в составе изделия, скрытых уязвимостей и каналов утечки информации, возможностей несанкционированных внешнего управления, искажения (потери) данных и в целом работоспособности (повреждения) изделия, а также несанкционированного считывания внутренней информации из изделия (в т.ч. по радиоканалу);

– подлинность (аутентичность), как достоверно подтвержденное отсутствие признаков контрафактной продукции;

– отсутствие недокументированных изменений (коррекций), внесенных в процессе ее разработки и/или производства и не верифицированных в установленном порядке (в результате типовых испытаний).

Совокупность перечисленных свойств являются критически необходимой для эффективного использования гражданской ЭКБ в целевых системах, однако в настоящее время она практически не охвачена системой стандартизации и государственного нормативного регулирования.

Отметим, что в стране накоплен значительный положительный опыт создания изделий ЭКБ оборонного назначения, которые по принципам разработки и производства являются заведомо доверенными, что обеспечивается их реализацией в соответствие с комплексом государственных военных стандартов «Климат-8» и общих технических условий на группы однородной продукции, а также специальными проверками. Однако номенклатура оборонной ЭКБ не может являться конкурентоспособной основой для создания широкого спектра гражданской продукции – прежде всего, по многократной избыточности своих технических требований и финансово-экономическим характеристикам. Накопленный опыт обеспечения доверенности при реализации оборонной ЭКБ относится в основном к унифицированным комплектующим изделиям невысокой степени сложности и не ориентирован на аппаратурно-ориентированные системы-на-кристалле и системы-в-корпусе (СнК/СвК) с распределенным циклом создания, что требует значимого переосмысления и радикальной коррекции методов и подходов обеспечения эффективной реализации и конкурентоспособности современных гражданских доверенных изделий.

ОТ ГЛАВНОГО РЕДАКТОРА

Современная доверенная ЭКБ гражданского назначения, создаваемая в рамках реализации Концепции развития электронной отрасли, является перспективной для внутреннего рынка при следующих ее особенностях:

– ЭКБ как правило относится к аппаратурно-ориентированным изделиям (или изделиям частного применения) и предназначена для нужд конкретных групп потребителей (т.е. не является унифицированной);

– значительная часть номенклатуры ЭКБ характеризуется широким разнообразием при относительно невысокой тиражности;

– процесс создания ЭКБ является распределенным: разработка в дизайн-центрах (фаблесс) на основе готовых IP-блоков, изготовление на кремниевых фабриках, верификация, тестирование, испытания и сертификация готовых изделий в испытательных и сертификационных центрах и «тестовых домах»;

– процесс разработки и изготовления, комплектность документов, объем тестирования, сама необходимость испытаний ЭКБ определяются разработчиком/изготовителем/потребителем на основе технико-экономической целесообразности, и практически не регламентированы нормативными документами;

– сертификация ЭКБ проводится в соответствии с отраслевыми добровольными системами качества, как правило, не учитывающими особенности технических требований к электронной продукции;

– конструктивное исполнение ЭКБ в виде СнК/СвК, в том числе в виде 2,5D- и 3D-микромодулей и сборок на чиплетах;

– критически важным свойством гражданской ЭКБ является конкурентоспособность на основе минимизации стоимости и сроков реализации проектов с учетом обеспечения доверенности.

Перечисленные особенности такой гражданской ЭКБ и РЭА на ее основе (не относящейся к СЗИ и ВВСТ) для обеспечения «доверенности» требуют проведения комплекса научно-технических мероприятий и государственного нормативного регулирования на всех этапах жизненного цикла от задания технических требований, разработки, производства, поставки до входного контроля и эксплуатации изделий, особенно, создаваемых в рамках государственных или частно-государственных проектов с привлечением бюджетных средств.

Искренне надеюсь, что наш журнал «Безопасность информационных технологий», станет авторитетной коммуникационно-дискуссионной площадкой для создателей и потребителей доверенной электроники, внесет значимый вклад в развитие и информационное обеспечение этого очень актуального, перспективного и наукоемкого направления, являющегося фундаментом информационно-технологической независимости и безопасности страны, основой для радикального увеличения внутреннего спроса на отечественную электронную продукцию в условиях цифровой трансформации экономики.

Главный редактор Александр Ю. Никифоров
доктор технических наук, профессор
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия

Editor in chief Alexander Yu. Nikiforov
Doctor of Technical Sciences, Professor
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: aynik@spels.ru, https://orcid.org/0000-0002-2427-663X

Вячеслав М. Барбашов[1], Николай С. Трушкин[2], Виталий Г. Иваненко[3]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]*e-mail: VMBarbashov@mephi.ru, https://orcid.org/0000-0001-7136-415X*
[2]*e-mail: NSTrushkin@mephi.ru, https://orcid.org/0000-0003-2407-084X*
[3]*e-mail: VGIvanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501*

СТАТИЧЕСКИЕ И ДИНАМИЧЕСКИЕ ХАРАКТЕРИСТИКИ ИНТЕГРАЛЬНОЙ ОЦЕНКИ РАДИАЦИОННОЙ СТОЙКОСТИ БИС АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2022.1.02

Аннотация. В настоящее время наблюдается тенденция использования аппаратных средств защиты информации (СЗИ) в экстремальных условиях эксплуатации, в частности, при наличии мощного радиационного излучения. В связи с этим актуализируется проблема оценки устойчивости работы СЗИ, которая определяется радиационной стойкостью входящих в их состав больших цифровых интегральных схем (БИС). В настоящей работе рассмотрены методы оценки радиационной стойкости БИС в виде статических и динамических отказов, определяемых на основе функционально-логического моделирования БИС в условиях ионизирующего излучения. Показано, что в ряде случаев потери информационной устойчивости работы СЗИ характерны детерминированные и недетерминированные отказы при воздействии дестабилизирующего фактора. Предложены методы прогнозирования радиационной стойкости БИС, которые основаны на моделях нечеткого цифрового и вероятностного надежностного автоматов. В первом случае, поведение аппаратных СЗИ определяется конкретным соотношением радиационно-чувствительных параметров его элементов, во втором, статистическим разбросом моментов переключения приводящих к изменению логики работы однотипных образцов. Причем характер их изменения при облучении зависит от многих факторов, включая тип излучения, его интенсивность и спектр, вид критериального параметра характеризующего радиационную стойкость БИС и режим работы. Анализ такого сопоставления является необходимым этапом для оценки радиационной стойкости БИС, что позволяет сформулировать подходы к анализу сигнальных сбоев цифровых устройств позволяющих обеспечить защиту информации.

Ключевые слова: аппаратные средства, детерминированные и недетерминированные отказы, защита информации, интегральная оценка, нечеткая вероятность, радиационная стойкость, устойчивость.

Для цитирования: БАРБАШОВ, Вячеслав М.; ТРУШКИН, Николай С.; ИВАНЕНКО, Виталий Г. СТАТИЧЕСКИЕ И ДИНАМИЧЕСКИЕ ХАРАКТЕРИСТИКИ ИНТЕГРАЛЬНОЙ ОЦЕНКИ РАДИАЦИОННОЙ СТОЙКОСТИ БИС АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 9–16, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1405. DOI: http://dx.doi.org/10.26583/bit.2022.1.02.

Vyacheslav M. Barbashov[1], Nikolai S. Trushkin[2], Vitaliy G. Ivanenko[3]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]*e-mail: VMBarbashov@mephi.ru, https://orcid.org/0000-0001-7136-415X*
[2]*e-mail: NSTrushkin@mephi.ru, https://orcid.org/0000-0003-2407-084X*
[3]*e-mail: VGIvanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501*

Static and dynamic characteristics of the integrated assessment of the radiation resistance of LSI of the hardware means of information protection

DOI: http://dx.doi.org/10.26583/bit.2022.1.02

Abstract. Currently, there is a tendency to use the hardware means of information protection in extreme operating conditions, in particular, in the presence of powerful radiation. In this regard, the problem of

assessing the stability of the hardware means of information protection operation is being updated, which is determined by the radiation resistance of the large digital integrated circuits (LSI) that make up them. Methods for ensuring information security in the form of static and dynamic characteristics, which are based on the use of functional-logical modeling of large digital integrated circuits (LSI) under the influence of ionizing radiation, are considered. It is shown that in some cases, information security is characterized by deterministic and non-deterministic failures when exposed to ionizing radiation. Methods for predicting the information security of LSI under the influence of ionizing radiation are proposed, which are based on models of fuzzy digital and probabilistic reliability automata. In the first case, the behavior of complex devices is determined by the specific ratio of radiation-sensitive parameters of the elements, in the second case by the statistical spread of switching moments leading to changes in the logic of the same type of sample. Moreover, the nature of their changes during irradiation depends on many factors, including the type of radiation, its intensity and spectrum, the type of criterion parameter that characterizes the radiation resistance of the LSI, and the mode of operation of the microcircuits.Conducting such a comparison is a necessary step for an adequate assessment of the radiation resistance of the LSI, which allows us to develop a procedure for analyzing the resistance of digital devices.
Keywords: hardware, deterministic and non-deterministic failures, information protection, integral estimation, fuzzy probability, radiation resistance, stability.
For citation: BARBASHOV, Vyacheslav M.; TRUSHKIN, Nikolai S.; IVANENKO, Vitaliy G. Static and dynamic characteristics of the integrated assessment of the radiation resistance of LSI of the hardware means of information protection. IT Security (Russia), [S.l.], v. 29, n. 1, p. 9–16, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1405. DOI: http://dx.doi.org/10.26583/bit.2022.1.02.

Введение

В настоящее время актуальной задачей обеспечения безопасности объектов критической информационной инфраструктуры (КИИ), функционирующей в экстремальных условиях эксплуатации, является устойчивость аппаратных средств управления, в том числе, комплексов защиты информации. В свою очередь этот показатель во многом определяется безотказностью работы сложных БИС, устойчивых к воздействию дестабилизирующих факторов, например, радиационного излучения.

Создание подобных БИС невозможно без активного использования функционально-логического моделирования, обеспечивающего необходимую адекватность описания и точность расчетов. В [1] рассмотрены сигнальные сбои работы логических элементов и устройств на их основе при воздействии ионизирующего излучения (ИИ). В данной работе сделана попытка выделить параметрические отказы обусловленные изменением фаз сигналов, отвечающие за временные характеристики работы цифровых устройств, с учетом воздействия ИИ. Известно, что увеличение тактовой частоты приводит к возникновению временных сбоев логических элементов из-за разброса задержек сигналов при переключении. В результате моделирования цифровых устройств выявляются, как известно [2, 3], сигнальные сбои, в узлах, в которых могут произойти статические или динамические отказы, что в результате состязания сигналов при работе реального устройства способны привести к сигнальным сбоям логических элементов при воздействии ИИ.

При этом для оценки реального характера радиационного поведения сложной электронной системы целесообразно получить количественные характеристики вероятности сбоев и на этой основе оценить допустимые ограничения.

1. Моделирующие среды описания сигнальных сбоев логических элементов при воздействии ионизирующего излучения

Следует отметить, что критические состязания существенно зависят от логики и структуры устройства. Однако статические и динамические риски сбоев в большей степени зависят от задержек срабатывания логических элементов $t_з^{10}$, $t_з^{01}$.

В логическом элементе задержки распределены статистически по законам φ_{10} и φ_{01}. Функции φ таковы, что на границах и за пределами такта каждая из них равна «0», унимодальные и не обязательно симметричные [4].

В зависимости от соотношения величин $t_з^{10}$, $t_з^{01}$ логический элемент по-разному переключается. Для элемента И-НЕ при воздействии сигналов h и ε возможны переключательные характеристики, которые приведены на рис. 1.

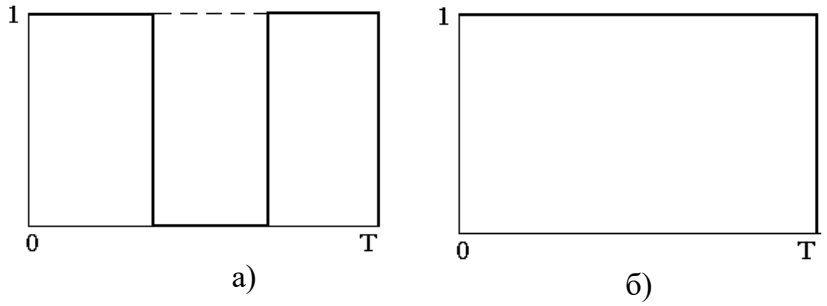


Рис. 1. Переключательные характеристики логического элемента И-НЕ при $t^{10} > t^{01}$ а) и $t^{10} < t^{01}$ б)
Fig. 1. Switching characteristic of the logic element AND-NOT at $t^{10} > t^{01}$ а) and at $t^{10} < t^{01}$ б)

Для элемента ИЛИ-НЕ аналогично получаются дуальные инверсные характеристики. Очевидно, что для однородного комбинационного блока из элементов И-НЕ, в котором превалируют элементы с характеристикой а), вероятность статистического риска сбоя резко возрастает. В исходном состоянии, при отсутствии воздействия ИИ, количество логических элементов с характеристиками а) и б) примерно одинаково и вероятность статического риска сбоев в основном зависит от вектора начального воздействия и логической структуры схемы. Хорошо известны методы нейтрализации статических и динамических рисков сбоя, но они малоэффективны при воздействии ИИ, когда начинают преобладать задержки определенного перехода. Приведенные экспериментальные данные в литературе [5] показывают, что возможны три случая появления таких задержек:

(1) начинает преобладать задержка сигнала h,

(2) начинает преобладать задержка сигнала ε,

(3) при дальнейшем росте поглощенной дозы ИИ сначала преобладает п.п (1), а затем п.п (2).

В случае (1) увеличивается количество элементов И-НЕ с характеристикой, показанной на рис. 1,а. Условно такие элементы назовем μ – элементами, их логика становится семизначной, если ввести дополнительные элементы множества модальностей. В этом случае в 7-мизначной логике для элемента И-НЕ таблицы истинности приведены на рис. 2,а, а для элемента ИЛИ-НЕ – на рис. 2,б.

В таблицах на рис. 2 через μ обозначена модальность μ элемента, а через «$\bar{\mu}$» инверсная модальность. Модальность «х» проставляется в случае разных функций переключения, или если число переключений логического элемента больше 2.

В случае, когда число переключений больше 2 переключательная характеристика для логического элемента И-НЕ приведена на рис. 1,б, а соответствующая таблица истинности – на рис. 2,а. Для логического элемента ИЛИ-НЕ таблица истинности приведена на рис. 2,б.

	0	ε	x	h	μ	$\bar{\mu}$	1
0	1	1	1	1	1	1	1
ε	1	h	x	μ	x	x	h
x	1	x	x	x	x	x	x
h	1	μ	x	ε	x	x	ε
μ	1	x	x	x	x	μ	$\bar{\mu}$
$\bar{\mu}$	1	x	x	x	μ	x	μ
1	1	h	x	ε	$\bar{\mu}$	μ	0

а)

	0	ε	x	h	μ	$\bar{\mu}$	1
0	1	h	x	ε	$\bar{\mu}$	μ	0
ε	h	h	x	0	x	x	0
x	x	x	x	x	x	x	0
h	ε	0	x	ε	x	x	0
μ	$\bar{\mu}$	x	x	x	x	$\bar{\mu}$	0
$\bar{\mu}$	μ	x	x	x	$\bar{\mu}$	x	0
1	0	0	0	0	0	0	0

б)

Рис. 2. Таблицы истинности логических элементов И-НЕ а) и ИЛИ-НЕ б) в 7-мизначной логике
Fig. 2. Tables of the truth of logical elements in 7-digit logic AND-NOT -a), OR-NOT- b)

Для случая, сигнального сбоя логического элемента показанного на рис. 3 при увеличении поглощенной дозы логические состояние переходят с одной логики на другую. При этом возникает нечеткая ситуация и в этом случае при моделировании состояний логического элемента схема рассчитывается по различным логикам, что позволяет при сравнении с экспериментом выявлять нечеткую вероятность динамических сбоев. При этом оценивается нечеткая вероятность сбоя по элементу по двум крайним ситуациям (1) и (2) [6].

	0	ε	x	h	1
0	1	1	1	1	1
ε	1	h	x	μ	h
x	1	x	x	x	x
h	1	1	x	ε	ε
1	1	h	x	ε	0

а)

	0	ε	x	h	1
0	1	h	x	ε	0
ε	h	h	x	0	0
x	x	x	x	x	0
h	ε	0	x	ε	0
1	0	0	0	0	0

б)

Рис. 3. Таблицы истинности логических элементов И-НЕ а) и ИЛИ-НЕ б)
Fig. 3. The truth tables of the logic elements AND-NOT - a), OR-NOT - b)

Пусть ν – относительная задержка $t_з^{10}$ сигнала h, ξ относительная задержка $t_з^{01}$ сигнала ε. Тогда ($\nu - \xi$) критериальная функция на множестве [0, 1] при условии, что $\nu \geq \xi$.

Кроме указанных свойств функций распределения φ_1 и φ_2 примем, что они бесконечно дифференцируемые и вне отрезка [0, 1] тождественно равны 0, и кроме этого: $\int_{-\infty}^{+\infty} \varphi_1 = 1$ и $\int_{-\infty}^{+\infty} \varphi_2 = 1$. Этим условиям отвечает, нормальный закон распределения Гаусса.

Нечеткую вероятность в этом случае можно записать в следующем виде:

$$\tilde{P}_{10} = \iint_{\Omega} (\nu - \xi)\varphi_1 \ (\nu) \cdot \varphi_1(\xi) d\nu d\xi \,, \tag{1}$$

где $\Omega = \{[0,1] \times [0,1], \ \nu \geq \xi\}$, область Ω приведена на рис. 4.

Интеграл (1) можно преобразовать к виду:

$$\tilde{P}_{10} = \int_0^1 \nu \, \varphi_1 (\nu) \int_0^{\nu} \varphi_2 \ (\xi) d\xi \, d\nu - \int_0^1 \varphi_1 \ (\nu) \int_0^{\nu} \xi \varphi_2 (\xi) d\xi \, d\nu. \tag{2}$$

Учитывая свойства функций φ_1 и φ_2, возможно преобразовать выражения (2):

$$\tilde{P}_{10} = \int_{-\infty}^{+\infty} \nu \, \varphi_1 (\nu) \int_{-\infty}^{\nu} \varphi_2 \ (\xi) d\xi \, d\nu - \int_{-\infty}^{+\infty} \varphi_1 \ (\xi) d\xi \int_{-\infty}^{+\infty} \xi \varphi_2 (\xi) d\xi + \\ + \int_{-\infty 0}^{+\infty} \nu \, \varphi_2 (\nu) \int_{-\infty}^{\nu} \varphi_1 \ (\xi) d\xi \, d\nu. \tag{3}$$

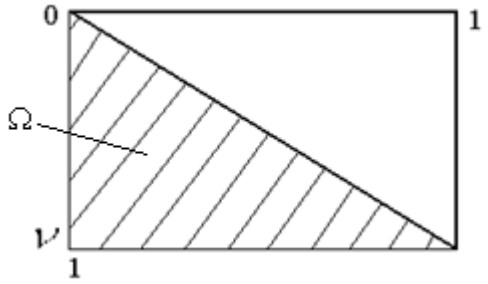


Рис. 4. Область интегрирования $\widetilde{P_{10}}$
Fig. 4. The integration area $\widetilde{P_{10}}$

При записи (3) видно, что в первом интеграле $\nu\cdot\int_{-\infty}^{\nu}\varphi_2\,(\xi)\,d\nu$ есть, по сути, нечеткая вероятность достижение параметра $(\xi \to \nu)$. Тогда эту функцию обозначим через $\widetilde{P_2}(\nu)$. Так как $\widetilde{P_2}(\nu)$ локально интегрируема на любом конечном отрезке из $(-\infty, +\infty)$, то данный интеграл есть не что иное, как функционал на D – пространстве φ Шварца [1] функций φ_1. Но так как φ_1 и φ_2 имеют одинаковые свойства, то их можно объединить в одно D-пространство φ. Следовательно, первый интеграл (3) можно записать в виде $< \widetilde{P_2}(\nu), \varphi >$ [7].

Второе слагаемое в (3) есть математическое ожидание ξ или максимальная нечеткая вероятность ξ, которую обозначим через M_2. Тот факт, что объекты теории вероятности могут совпадать с нечеткими характеристиками, объясняется линейной формой критериальной функции.

Третий интеграл в (3) аналогично интерпретируется как функционал по пространству φ нечеткой вероятности ν, обозначаемой через $\widetilde{P_1}(\nu)$. Таким образом, с учетом всех обозначений и допущений выражение (3) примет следующий вид:

$$\widetilde{P_{10}} = < \tilde{P}_1(\nu),\ \varphi > + < \tilde{P}_2(\nu),\ \varphi > - M_2. \qquad (4)$$

При конкретных расчетах в первом слагаемом (4) подставляется в $\widetilde{P_1} \to \varphi_1$, а вместо $\varphi \to \varphi_2$. Во втором слагаемом в $\widetilde{P_2} \to \varphi_2$, а вместо $\varphi \to \varphi_1$. При вычислении M_2 в соответствующем интеграле подставляется φ_2.

Формула (4) позволяет оценить глобально нечеткую вероятность по всем распределениям φ, удовлетворяющим вышеуказанным условиям.

Функции φ в общем случае могут быть вида:υ

$$\varphi = A \cdot e^{-\Psi(x-\tau)},$$

где A – нормировка, $\tau \in (0,1)$– центр распределения.

При этом функция Ψ должна удовлетворять следующим условиям:

1. Ψ – бесконечно дифференцируема
2. $\Psi(x-\tau) \underset{\substack{x\to 0\\ x\to 1}}{\to} +\infty;$
3. $\lim\limits_{\substack{x\to 0\\ x\to 1}} \left[\Psi^{(к)}(x-\tau)\cdot e^{-\Psi}\right] = 0, \quad к = 1,2,\ldots;$ (5)
4. $\Psi^1(x-\tau) = \begin{cases} 0, & x = \tau \\ \neq 0, & x \neq \tau \end{cases};$
5. $\Psi(0) = 0.$

Вне промежутка $(0, 1)$ функция φ тождественно равна 0. Следовательно, носитель у функции φ одинаковый [0, 1]. В пространстве D Лорана Шварца носители функций φ не обязательно одинаковые. Так, что в данном случае при выполнении условий (5) и фиксации носителя можно считать полученное пространство подпространством пространства D. В этом случае, так как функции φ не обязательно симметричные, то, подбирая подходящую функцию Ψ, можно аппроксимировать экспериментальные распределения конкретно для каждого логического элемента.

2. Экспериментальные исследования

Радиационная стойкость КМОП ИС как правило зависит от выполнения функционально-логической функции элемента: наименьшее изменение $t_{з.р}$ наблюдается у логического элемента НЕ рис. 5 (2), максимальные – у логического элемента 2И-НЕ рис. 5 (1) [8, 9].

Немонотонный характер зависимостей $t_{з.р}(D)$ у разных типов ИС и БИС указывает на существенную неоднородность стойкости логических элементов. В частности КМОП ИС определяются двумя процессами, которые приводят к нарушению функционирования: потеря управления транзисторами с каналом р-типа приводит к увеличению $t_{з.р}$ рис. 6 (2); потеря управления транзисторами с каналом n-типа приводит к уменьшению $t_{з.р}$ рис. 6 (1). В связи с этим, такая неоднородность приводит к отличию в радиационной стойкости внутренних узлов БИС и выражается в зависимости от функционального режима работы и внутренней организации, что подтверждается теоретически и экспериментально практически на всех типах БИС [10–12].

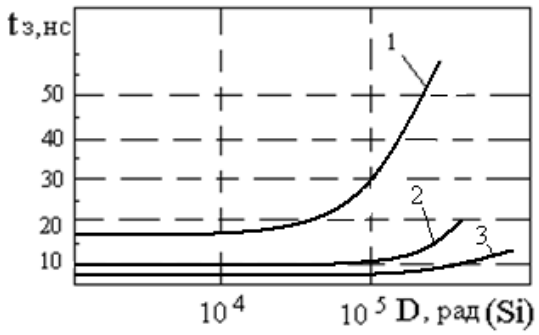


Рис. 5. Зависимость времени задержки КМОП ИС от дозы γ – облучения ^{60}Co: 1 – схема 2И-НЕ (E=5 В); 2 – схема НЕ (5 В); 3 – схема НЕ (10 В)
Fig. 5. Dependence of the delay time of CMOS IC onγ – radiation dose ^{60}Co:
1 – 2AND-NOT circuit (E=5 V); 2 – NOT circuit (5 V); 3 – NOT circuit (10 V)

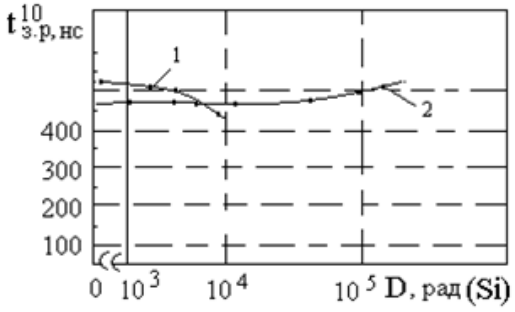


Рис. 6. Зависимость времени задержки в микропроцессоре 1802 – 1 и его радиационно-стойком варианте от поглощенной дозы – 2
Fig. 6. Dependence of the propagation delay time on the absorbed dose in the 1802 – 1 microprocessor and in its radiation-resistant version-2

Как видно на рис. 5, для ИС выполненных по КМОП технологии, наименьшие изменения времени задержки наблюдаются у логических элементов НЕ (2), а максимальные изменения – у элементов 2И-НЕ (1) [13]. Для БИС, выполненных по МОП технологии, изменения быстродействия связаны с основным радиационно-чувствительным параметром – пороговым напряжением транзистора. В зависимости от особенностей технологического

исполнения быстродействие может возрастать или уменьшаться при облучении. Так, в микропроцессоре 1802, изготовленном по КМОП технологии, рост поглащенной дозы ИИ приводит к уменьшению пороговых напряжений n-МОП транзисторов, что вызывает снижение времени задержки распространения сигнала, рис. 6 (1) [14]. В радиационно-стойком исполнении КМОП микропроцессоре, где повышена стойкость n-МОП транзисторных структур, существенную роль играет увеличение пороговых напряжений p-МОП транзисторов при увеличении поглощенной дозы. На рис. 6 (2) видно, что если поглощенная доза превышает 10^5рад (Si), то происходит рост $t_{\text{з.р}}^{10}$.

Заключение

В заключение следует отметить, что при оценке стойкости функционирования БИС в условиях радиационного облучения необходимо учитывать соотношение радиационно-чувствительных параметров элементов БИС и влияние их статистического разброса. Соотношение между функцией распределения плотности вероятности разброса и критериальной функцией принадлежности определяет, в конечном итоге, целесообразность использования функционально-логических моделей радиационного поведения БИС применительно к каждому конкретному критическому процессу.

Такое сопоставление является необходимым этапом общей процедуры анализа стойкости БИС и, следовательно, оценки устойчивости функционирования СЗИ в экстремальных условиях эксплуатации. При этом следует иметь в виду, что параметры функции распределения, характеризующие неконтролируемые статистические процессы сами по себе являются также зависимыми от радиации.

СПИСОК ЛИТЕРАТУРЫ:

1. Шварц Л. Математические методы для физических наук. М.: Мир, 1965. – 412 с.
2. Барбашов В.М. Моделирование функциональных отказов цифровых систем при воздействии радиации. Датчики и системы. 2011, № 6, с. 29–34. URL: https://www.elibrary.ru/item.asp?id=16497840 (дата обращения: 23.05.2021).
3. Gretzer G. General Lattice Theory. 1978. Publisher: Academic Press, Inc., New York, Birkhäuser Verlag, Basel, Akademie Verlag, Berlin ISBN: 0-12-295750-4. URL: https://www.researchgate.net/publication/258514502_General_Lattice_Theory(датаобращения: 23.05.2021).
4. Барбашов В.М., Трушкин Н.С. Взаимосвязь вероятностных и порядковых моделей при моделировании функциональной безопасности БИС. Безопасность информационных технологий, [S.l.], т. 15, № 3, с. 90–95, 2008. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/987 (дата обращения: 23.05.2021).
5. Барбашов В.М., Трушкин Н.С. Функционально-логическое моделирование качества функционирования ИС при воздействии радиационных и электромагнитных излучений// Микроэлектроника. 2009, т. 38, № 1, с. 34–47. URL: https://www.elibrary.ru/item.asp?id=11663446 (дата обращения: 26.05.2021).
6. Барбашов В.М., Трушкин Н.С., Калашников О.А. Детерминированные и недетерминированные модели отказов бис при воздействии радиации. Микроэлектроника. Т. 44, № 5, с. 312–315, 2015. DOI: http://dx.doi.org/10.7868/S0544126915050038.
7. Нечеткие множества и теория возможностей // Под ред. Р.Р. Ягера. М.: Радио и связь, 1986. – 408 с. URL: http://www.bookre.org/reader?file=479837 (дата обращения: 23.05.2021).
8. Gibbon C.F., Hobing D.Y., Flores R.S. A Radiation-Hard Silicon Gate Bulk CMOS Cell Family. IEEE Trans.1980, vol. NS-27, no. 6, p. 1712–1715. DOI: http://dx.doi.org/10.1109/TNS.1980.4331093.
9. Радиационные методы в твердотельной электронике/В.С. Вавилов, Б.М. Горин, Н.С. Данилин и др. М.: Радио и связь, 1990. – 184 с. URL: https://search.rsl.ru/ru/record/01001538235 (дата обращения: 23.05.2021).
10. King E.E., Martin R.L. Effects of total dose ionizing radiation on the 1802 microprocessor. IEEE Trans., 1977, NS-24, no. 6, p. 2172–2176. DOI: http://dx.doi.org/10.1109/TNS.1977.4329186.
11. Проектирование устройств вычислительной техники с учетом радиационных воздействий. Е.Р. Аствацатурьян, О.Н. Голотюк, Ю.А. Попов, П.К. Скоробогатов и др. М.: Изд. МИФИ, 1985. – 84 с. URL: https://search.rsl.ru/ru/record/01001301654 (дата обращения: 23.05.2021).

12. Sogoyan A.V., Chumakov A.I., Nikiforov A.Yu. Method for Predicting CMOS Parameter Degradation Due to Ionizing Radiation with Regard to Operating Time and Conditions. Russian Microelectronics. 1999, vol. 28, no. 4, p. 224–235. URL: https://www.elibrary.ru/item.asp?id=13747675 (дата обращения: 23.05.2021).
13. Kalashnikov O.A. and NikiforovA.Y. TID behavior of complex multifunctional VLSI devices, 2014 29th International Conference on Microelectronics Proceedings – MIEL 2014, p. 455–458. DOI: http://dx.doi.org/10.1109/MIEL.2014.6842189.
14. Boychenko D.V., Kessarinskiy L.N., Pechenkina. The influence of the electrical conditions on total dose behavior of the analog switches.2011 12th European Conference on Radiation and Its Effects on Components and Systems (2011): 822-824. DOI: http://dx.doi.org/10.1109/RADECS.2011.6131340.

REFERENCES:

[1] Schwartz L. Mathematical methods for the physical Sciences. M.: Mir, 1965 – 412 p. (in Russian).
[2] Barbashov V.M. Simulation of functional failures of digital systems when exposed to radiation. Sensors and systems. 2011, no. 6, p. 29–34. URL: https://www.elibrary.ru/item.asp?id=16497840 (accessed: 23.05.2021) (in Russian).
[3] Gretzer G. General Lattice Theory. 1978. Publisher: Academic Press, Inc., New York, Birkhäuser Verlag, Basel, Akademie Verlag, Berlin ISBN: 0-12-295750-4. URL: https://www.researchgate.net/publication/258514502_General_Lattice_Theory(accessed: 23.05.2021).
[4] Barbashov V.M. Trushkin N.S. With. The relationship of probabilistic and ordinal models in the modeling of functional safety LSI. IT Security (Russia), [S.l.], vol. 15, no. 3, p. 90–95, 2008. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/987 (accessed: 23.12.2021) (in Russian).
[5] Barbashov V.M. Trushkin N.S. With. Functional-logical modeling of the quality of operation of the IC when exposed to radiation and electromagnetic radiation. Microelectronics. 2009, vol. 38, no. 1, p. 34–47. URL: https://www.elibrary.ru/item.asp?id=11663446 (accessed: 23.05.2021) (in Russian).
[6] Barbashov V.M., Trushkin N.S., Kalashnikov O.A. Deterministic and nondeterministic failure models of lsi circuits exposed to radiation. Russian Microelectronics. Vol. 44, no. 5, p. 312–315, 2015. DOI: http://dx.doi.org/10.7868/S0544126915050038 (in Russian).
[7] Fuzzy sets and the theory of possibilities. Edited by R.R. Jager. M.: Radio and Communications, 1986. – 408 p. URL: http://www.bookre.org/reader?file=479837 (accessed: 23.12.2021) (in Russian).
[8] Gibbon C.F., Hobing D.Y., Flores R.S. A Radiation-Hard Silicon Gate Bulk CMOS Cell Family. IEEE Trans. 1980, vol. NS-27, no. 6, p. 1712–1715. DOI: http://dx.doi.org/10.1109/TNS.1980.4331093.
[9] Radiation methods in solid-state electronics. V.S. Vavilov, B.M. Gorin, N.S. Danilin, etc. M.: Radio and Communications, 1990. – 184 p. URL: https://search.rsl.ru/ru/record/01001538235 (accessed: 23.05.2021) (in Russian).
[10] King E.E., Martin R.L. Effects of total dose ionizing radiation on the 1802 microprocessor. IEEETrans., 1977, NS-24, no. 6, p. 2172–2176. DOI: http://dx.doi.org/10.1109/TNS.1977.4329186.
[11] Design of computer equipment devices taking into account radiation effects. E.R. Astvatsaturyan, O.N. Golotyuk, Yu.A. Popov, P.K. Skorobogatov, et al. M.: MEPhI Publishing House, 1985. – 84 p. URL: https://search.rsl.ru/ru/record/01001301654 (accessed: 23.05.2021) (in Russian).
[12] Sogoyan A.V., Chumakov A.I., Nikiforov A.Yu. Method for Predicting CMOS Parameter Degradation Due to Ionizing Radiation with Regard to Operating Time and Conditions. Russian Microelectronics. 1999, vol. 28, no. 4, p. 224–235. URL: https://www.elibrary.ru/item.asp?id=13747675 (accessed: 23.05.2021).
[13] Kalashnikov O.A. and Nikiforov A.Y. TID behavior of complex multifunctional VLSI devices, 2014 29th International Conference on Microelectronics Proceedings - MIEL 2014, p. 455–458. DOI: http://dx.doi.org/10.1109/MIEL.2014.6842189.
[14] Boychenko D.V., Kessarinskiy L.N., Pechenkina D.V. The influence of the electrical conditions on total dose behavior of the analog switches. 2011 12th European Conference on Radiation and Its Effects on Components and Systems (2011): 822-824. DOI: http://dx.doi.org/10.1109/RADECS.2011.6131340.

Поступила в редакцию –25 мая 2021 г. Окончательный вариант – 17 февраля 2022 г.
Received –May 25, 2021. The final version – February 17, 2022.

Алексей Ю. Боровиков[1], Артем П. Карпов[2], Владимир Н. Пелин[3], Станислав Е. Кузнецов[4]
Пензенский филиал АО «Научно-технический центр «Атлас»,
пр–кт Победы, 69, Пенза, 440028, Россия
[1]e-mail: alexey_bau@mail.ru, https://orcid.org/0000-0002-3595-2533
[2]e-mail: atlas@atlas-pf.ru, https://orcid.org/0000-0002-3462-2153
[3]e-mail: atlas@atlas-pf.ru, https://orcid.org/0000-0003-4274-9047
[4]e-mail: atlas@atlas-pf.ru, https://orcid.org/0000-0003-0516-7806

СОЗДАНИЕ СПЕЦИАЛИЗИРОВАННОГО ДОВЕРЕННОГО УСТРОЙСТВА АНАЛИЗА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

DOI: http://dx.doi.org/10.26583/bit.2022.1.03

Аннотация. Целью работы является создание специализированного доверенного устройства анализа информации (СДУ АИ), предназначенного для контроля и фильтрации информации при управлении каналообразующими средствами в автоматизированной системе в защищенном исполнении, обрабатывающей информацию ограниченного доступа и имеющей возможность передачи информации по открытым (незащищенным от несанкционированного доступа) каналам связи. С развитием автоматизированных систем все большее значение приобретают автоматизация функций, в том числе управления каналообразующими средствами, безопасность обрабатываемой информации и оперативность выполняемых задач. При этом в автоматизированных системах в защищенном исполнении (АСЗИ) для организации оперативного автоматизированного управления каналообразующими средствами, как правило, требуется обеспечить взаимодействие сетей с различной степенью конфиденциальности обрабатываемой информации. Объектом исследования являются АСЗИ обрабатывающие информацию ограниченного доступа в одной сети и реализующие обмен информацией по открытым (незащищенным от несанкционированного доступа) каналам связи с другой сетью. Предметом исследования является оценка возможности применения СДУ АИ для обеспечения возможности сопряжения сетей с различной степенью конфиденциальности обрабатываемой информации, выполняющего функции контроля и фильтрации информации при управлении каналообразующими средствами. Разработана унифицированная архитектура СДУ АИ. Рассмотрены угрозы информационной безопасности, возникающие при реализации обмена информацией по открытым каналам связи. Предложен способ создания СДУ АИ на базе доверенной аппаратно-программной платформы, предназначенного для применения в АСЗИ для защиты от выявленных угроз информационной безопасности.

Ключевые слова: автоматизированная система в защищенном исполнении, доверенная аппаратно-программная платформа, каналообразующие средства, канал связи, защита информации, информационная безопасность, автоматизированное управление, фильтрация информации.

Для цитирования: БОРОВИКОВ, Алексей Ю. и др. СОЗДАНИЕ СПЕЦИАЛИЗИРОВАННОГО ДОВЕРЕННОГО УСТРОЙСТВА АНАЛИЗА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 17–29, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1408. DOI: http://dx.doi.org/10.26583/bit.2022.1.03.

Alexey Y. Borovikov[1], Artem P. Karpov[2], Vladimir N. Pelin[3], Stanislav E. Kuznecov[4]
Penza Branch of Atlas Scientific and Technical Center JSC,
Pobedy Avenue, 69, Penza, 440028, Russia.
[1]e-mail: alexey_bau@mail.ru, https://orcid.org/0000-0002-3595-2533
[2]e-mail: atlas@atlas-pf.ru, https://orcid.org/0000-0002-3462-2153
[3]e-mail: atlas@atlas-pf.ru, https://orcid.org/0000-0003-4274-9047
[4]e-mail: atlas@atlas-pf.ru, https://orcid.org/0000-0003-0516-7806

Method for creating a specialized trusted device for analyzing information in protected operational system

DOI: http://dx.doi.org/10.26583/bit.2022.1.03

Abstract. This work aims to create a specialized trusted information analysis device (SDU AI) designed to control and filter information when controlling channel-forming means in an automated system in a secure design that processes restricted access information and can transmit information over open (unprotected from unauthorized access) communication channels. With the development of automated systems, automation of functions, including the control of channel-forming means, the security of processed information and the efficiency of tasks are becoming increasingly important. At the same time, in automated systems in protected execution (ASZI), for the organization of operational automated control of channel-forming means, as a rule, it must ensure the interaction of networks varying degrees of confidentiality of the processed information. The object of the study is ASZI processing restricted access information in one network and implementing the exchange of information through open (unprotected from unauthorized access) communication channels with another network. The subject of the study is to assess the possibility of using SDU AI to ensure the possibility of interfacing networks with varying degrees of confidentiality of processed information, performing the functions of monitoring and filtering information when managing channel-forming means. A unified architecture of the SDU AI has been developed. The threats to information security arising from the implementation of information exchange through open communication channels are considered. A method for creating a SDU AI based on trusted hardware and software platform designed for use in the ASZI to protect against identified threats to information security is proposed.

Keywords: automated system in secure execution, trusted hardware and software platform, channel-forming means, communication channel, information protection, information security, automated management, information filtering.

For citation: BOROVIKOV, Alexey Y. et al. Method for creating a specialized trusted device for analyzing information in protected operational system. IT Security (Russia), [S.l.], v. 29, no. 1, p. 17–29, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1408. DOI: http://dx.doi.org/10.26583/bit.2022.1.03.

Введение

В настоящее время военно-промышленный комплекс Российской Федерации характеризуется ростом различного рода автоматизированных систем, разрабатываемых в интересах МО РФ и предназначенных для обработки информации ограниченного доступа (АСЗИ). Разработка и совершенствование таких систем с целью соответствия их современным требованиям по оперативности взаимодействия, автоматизации управления и обеспечения безопасности обрабатываемой информации является важнейшей задачей обеспечения обороноспособности страны и суверенитета государства.

Рассматриваемые автоматизированные системы в общем случае включают в себя сеть обработки информации ограниченного доступа (информация для служебного пользования, информация, содержащая сведения, составляющие государственную тайну, и др.) (далее – защищенная сеть) и сеть обработки общедоступной информации, в том числе обеспечивающая возможность обмена информацией по открытым (незащищенным от несанкционированного доступа) каналам связи (далее – открытая сеть).

Для обмена информацией ограниченного доступа по открытым каналам связи в АСЗИ используются средства криптографической защиты информации (СКЗИ). При этом, разрабатываемая АСЗИ должна удовлетворять требованиям нормативных документов МО РФ, предъявляемым к программному обеспечению и автоматизированным системам, а также требованиям нормативных документов ФСБ России в части корректного применения СКЗИ и получения разрешения на его эксплуатацию в АСЗИ.

При проектировании данных АСЗИ разработчику требуется обеспечить сопряжение открытой и защищенной сети АСЗИ и организовать оперативное автоматизированное управление каналообразующими средствами.

В данной работе рассматривается создание СДУ АИ, предназначенного для применения в АСЗИ при организации автоматизированного управления каналообразующими средствами, обеспечивающего защиту от возникновения угроз информационной безопасности при использовании СКЗИ в АСЗИ.

Типовая архитектура АСЗИ представлена на рис. 1.

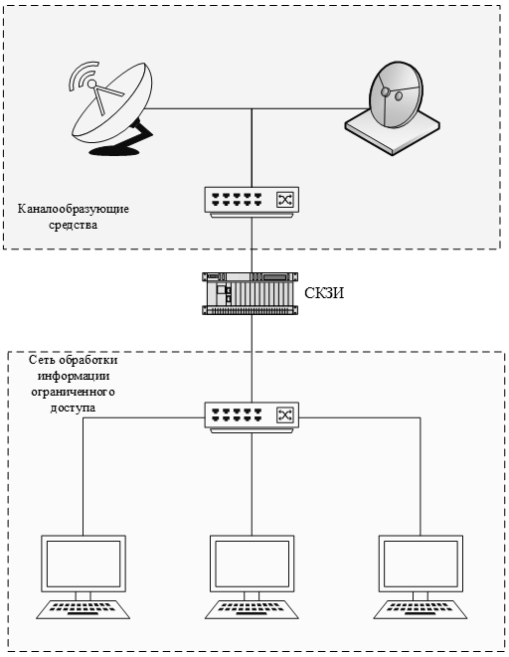


Рис. 1. Типовая архитектура АСЗИ
Fig. 1. Typical architecture of protected operational system

При типовой архитектуре построения АСЗИ требуется решение задач, связанных с необходимостью автоматизированного управления каналообразующими средствами: настройка технических средств (задание основных параметров работы, рабочей частоты, текущего времени и т.д.), сбор и централизованное хранение сведений о состоянии данных технических средств (включен, выключен, занят, в режиме ожидания и т.д.), прием и обработка инициативных сообщений (сообщения об ошибках, квитанции, сообщения об изменениях состояний и режимов работы и т.д.). Описание методов управления каналообразующими средствами в современных системах связи дано в [1], при этом в АСЗИ важным аспектом является обеспечение безопасной реализации данных методов.

Поскольку в рассматриваемой структуре построения АСЗИ все передаваемые из защищенной сети данные являются преобразованными с использованием СКЗИ, они не могут быть применены для управления каналообразующими средствами. Введение в состав открытой сети отдельного технического средства для выполнения функций управления каналообразующими средствами нецелесообразно по следующим причинам:

– технические средства (в частности – каналообразующие средства) из состава открытой сети АСЗИ, как правило, размещаются в условиях ограниченного пространства, в необслуживаемых и опломбированных помещениях (отсеках). Выделить в этих условиях

дополнительное автоматизированное рабочее место затруднительно, а иногда и невозможно;

– техническое средство из состава открытой сети не может взаимодействовать с защищенной сетью, следовательно, не может оперативно получать актуальные данные, необходимые для настройки каналообразующих средств (режим работы, рабочая частота и т.д.). Для обеспечения такого взаимодействия может быть использована внутренняя телефонная линия, но подобное взаимодействие не удовлетворяет требованиям оперативности, удобства использования и автоматизации, которым должны соответствовать современные автоматизированные системы [2].

Организация централизованного и автоматизированного управления каналообразующими средствам из защищенной сети является эффективным решением перечисленных проблем. Однако решение данной задачи осложняется появлением угроз безопасности информации, таких как попадание информации ограниченного доступа в открытые каналы связи и воздействие нарушителя по каналам связи с целью осуществления несанкционированного доступа к обрабатываемой информации.

Для предотвращения указанных угроз, при сопряжении сетей АСЗИ необходимо использовать специальные средства контроля и фильтрации информации. Такие средства не относятся ни к одной из рассматриваемых сетей, поскольку не обрабатывают информацию ограниченного доступа и не являются частью каналообразующих средств.

В настоящее время на российском рынке к изделиям, которые предназначены для сопряжения сетей разного уровня конфиденциальности, относятся межсетевые экраны и однонаправленные шлюзы.

Межсетевые экраны не могут быть применены для решения описываемой задачи, поскольку, в соответствии с действующими нормативными документами МО РФ и ФСБ России, использование данных технических средств для сопряжения защищенной сети с открытой сетью, имеющей подключение к открытым (незащищенным от несанкционированного доступа) каналам связи, не допускается.

Однонаправленные шлюзы в соответствии с действующими нормативными документами РФ могут применяться в составе АСЗИ, однако данные технические средства по определению не обеспечивают двунаправленное взаимодействие [3, 4] и, как следствие, не позволяют полноценно выполнять задачи по управлению и контролю состояния каналообразующих средств.

В связи с этим существующие в настоящее время изделия не могут быть использованы для реализации автоматизированного двунаправленного управления каналообразующими средствами в АСЗИ.

С целью реализации автоматизированного обмена информацией при управлении каналообразующими средствами в АСЗИ, учитывая архитектуру, протоколы информационного взаимодействия сетей, объемы передаваемой информации и ее содержание, предлагается разработать и применить СДУ АИ, в общем случае выполняющее следующие функции:

– контроль формата пакетов и значений в полях пакетов с управляющей информацией, между защищенной сетью и каналообразующими средствами открытой сети в соответствии с протоколом сетевого взаимодействия;

– возможность индивидуальной настройки (задания допустимых форматов и значений протокола взаимодействия) для каждой АСЗИ;

– защиту от передачи защищаемой информации из сети обработки информации ограниченного доступа;

– защиту от воздействий нарушителя по каналу связи с целью осуществления несанкционированного доступа к защищаемой информации.

1. Требования к математическому обеспечению СДУ АИ

Учитывая многообразие существующих и разрабатываемых АСЗИ, а также используемых в этих системах каналообразующих средств, разработка универсального устройства, обеспечивающего контроль и фильтрацию информации для всех существующих (и перспективных) сетевых и прикладных протоколов, невозможна. При этом, может быть определен и зафиксирован состав аппаратного обеспечения данного устройства, в то время как программное обеспечение, реализующее протокол межсетевого взаимодействия, должно предусматривать возможность конфигурации для каждой отдельно взятой АСЗИ, в которой используется СДУ АИ.

Ведущими специалистами ПФ АО «НТЦ «Атлас» был выполнен ряд инициативных работ, в рамках которых была создана унифицированная архитектура СДУ АИ, позволяющая, с одной стороны, реализовать целевые функции по фильтрации и контролю информации, а с другой – обеспечить возможность гибкой настройки и минимальной доработки программного обеспечения для применения СДУ АИ в конкретной АСЗИ.

СДУ АИ состоит из трех вычислительных модулей – абонентского (АВМ), канального (КВМ) и специального (СВМ), размещенных в едином конструктиве с учетом требований по стойкости к внешним воздействующим факторам. Абонентский и канальный модуль служат для сетевого взаимодействия с сопрягаемыми сетями АСЗИ и должны обеспечивать возможность настройки параметров межсетевого взаимодействия, а специальный вычислительный модуль выполняет основные функции защиты от попадания защищаемой информации в каналы связи и от воздействия нарушителя по каналам связи на технические средства АСЗИ. Такая архитектура позволяет унифицировать аппаратную часть устройства, обеспечить требуемый уровень защиты от угроз информационной безопасности за счет реализации основных мер защиты на специальном вычислительном модуле, а также обеспечить требуемую гибкость при проектировании СДУ АИ для различных АСЗИ. При встраивании СДУ АИ требуется доработка только программного обеспечения в соответствии с протоколом межсетевого взаимодействия АСЗИ.

Для применения СДУ АИ в конкретной АСЗИ необходимо тщательно проработать протокол взаимодействия сетей с учетом используемых каналообразующих средств. Данный протокол должен содержать полный перечень полей и значений управляющей информации и предусматривать возможность преобразования индивидуального формата управления каждым каналообразующим средством в универсальный формат межсетевого взаимодействия с СДУ АИ. Данные функции должны быть реализованы в программном обеспечении технических средств из состава АСЗИ.

При формировании универсального протокола межсетевого взаимодействия СДУ АИ и технических средств из состава АСЗИ необходимо руководствоваться следующими правилами:

– взаимодействие технических средств с СДУ АИ должно осуществляться по TCP или UDP-протоколу;

– поле данных в сетевых пакетах должно содержать ограниченный алфавит символов, который подлежит контролю на СДУ АИ. В качестве алфавита допускается использовать следующее множество: [a..z, 0..9, +,-,’ ’, !, ?, ., /,\, ^,%]. Мощность предложенного алфавита равна 46 и в соответствии с мерой Р. Хартли [5, 6] данный алфавит может быть закодирован $[\log_2(46)] + 1 = 6$ значащими битами. Таким образом, при

реализации злоумышленником описанных угроз информационной безопасности, стандартные символьные кодировки, требующие 8 бит (например, UTF-8, ASCII), 16 бит (например, UTF-16) и более, будут отбракованы на СДУ АИ;

– поле данных сетевых пакетов должно быть представлено в текстовом формате в виде «ключ-значение». Сетевые пакеты, которые содержат данные в бинарном формате или текстовую информацию в другом виде, будут отбракованы СДУ АИ. Таким образом, СДУ АИ будет блокировать потенциальные сетевые атаки нарушителя с использованием бинарных исполняемых файлов или текстовых программных скриптов. При этом представление «ключ-значение» является предпочтительным с точки зрения унификации протоколов управления разнообразных каналообразующих средств – для любого протокола можно определить исчерпывающий перечень ключей (команд) и соответствующий им перечень значений (параметров команд). В свободном доступе, в открытых исходных текстах содержится ряд библиотек для работы с подобными форматами (XML, JSON и т.д.). В связи с этим упрощается разработка программного обеспечения работы с управляющей информацией на технических средствах из состава АСЗИ для сопряжения с СДУ АИ [7, 8];

– поле данных сетевых пакетов должно содержать контрольную сумму, которая подлежит проверке на СДУ АИ. Контрольные суммы сформированных данных гарантируют их неизменность и защищают от случайного попадания информации ограниченного доступа в сетевые пакеты во время их доставки до СДУ АИ. В качестве контрольной суммы может быть использована одна из реализаций стандарта CRC32 [9, 10].

Формат пакета, сформированного в соответствии с рассмотренным протоколом взаимодействия, приведен на рис. 2.

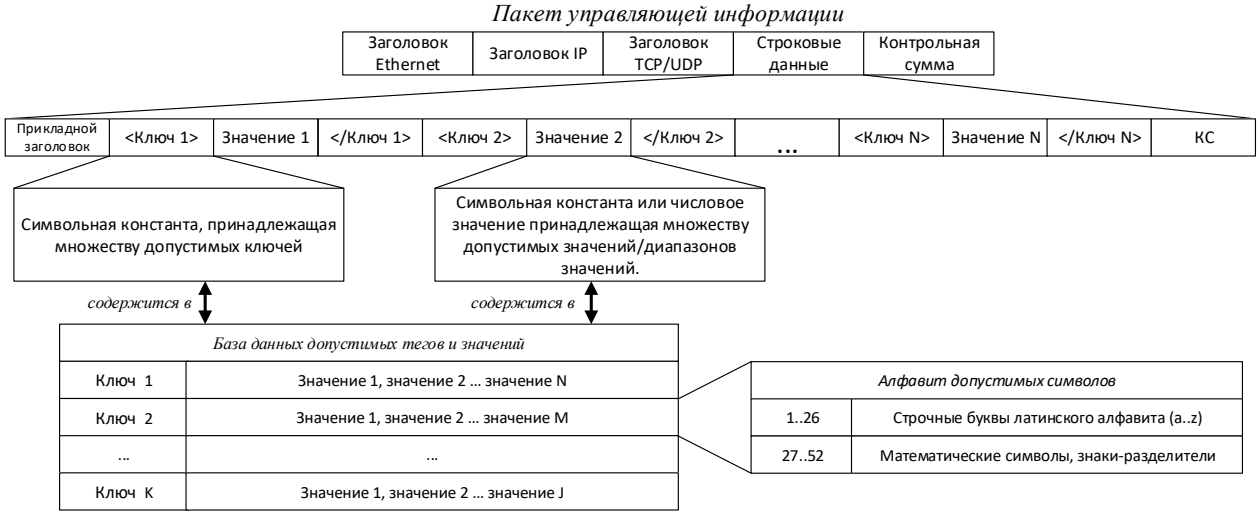


Рис. 2. Формат пакета управляющей информации
Fig. 2. Controlling information packet format

При реализации описанного протокола взаимодействия функции СДУ АИ можно свести к контролю соответствия передаваемых данных рассмотренному протоколу. В этом случае в АСЗИ защита от попадания информации в каналы связи и от воздействия нарушителем будет обеспечиваться за счет:

– контроля корректности адресной информации пакета с управляющей информацией;

– контроля корректности контрольной суммы пакета;

– контроля наличия в пакетах только данных в формате строк;

– контроля корректности контрольной суммы поля данных;

– контроля соответствия всех символов передаваемой строки допустимому алфавиту;

– контроля соответствия всех тегов и значений (диапазонов значений) передаваемых данных значениям, определенным в протоколе взаимодействия.

Пакеты с информацией ограниченного доступа, нештатно (за счет неисправностей, сбоев и ошибочных действий обслуживающего персонала) попадающие в СДУ АИ, будут отбракованы, равно как и пакеты с вредоносным программным обеспечением, которые могут быть сформированы и переданы нарушителем по каналам связи.

2. Требования к аппаратно-программному обеспечению СДУ АИ

Для обеспечения соответствия СДУ АИ и реализуемых им функций по защите информации уровню доверия, достаточному для сопряжения сетей АСЗИ, СДУ АИ должно удовлетворять следующим требованиям [11]:

– наличие конструкторской (схемы электрические принципиальные, схемы электрические подключений, габаритные и сборочные чертежи) и эксплуатационной документации (паспорт, руководство по эксплуатации) на аппаратную платформу;

– наличие исходного кода, программной документации и отсутствия опасных функциональных возможностей во встроенном программном обеспечении аппаратной платформы;

– применение сертифицированных по требованиям безопасности информации общесистемного, прикладного и специального программного обеспечения по соответствующему уровню контроля отсутствия недекларированных возможностей;

– применение сертифицированных аппаратно-программных или программных средств защиты информации для обеспечения невозможности работы несанкционированных пользователей и замкнутости программной среды.

– выполнение организационно-режимных и технических мер защиты информации от несанкционированного доступа.

Как показано в [12] при проектировании СДУ АИ выполнение указанных требований может быть обеспечено за счет:

– разработки на базе доверенной аппаратно-программной платформы отечественного производства, например, вычислительный блок БВ001 ЦИАТ.467444.251 (производитель ПФ АО «НТЦ «Атлас») на базе модуля процессора СРС1311 (производитель ЗАО «НПФ «Доломант») с загрузчиком операционных систем Горизонт ЦИАТ.00169-01 (ЗОС Горизонт), выполняющим функции ПО BIOS и реализующим механизмы защиты от несанкционированного доступа на этапе начального старта до загрузки операционной системы. Данный загрузчик реализует комплекс мер защиты от несанкционированного доступа к ПО, в том числе от атак на уровне базовой системы ввода/вывода и решает задачу построения доверенной вычислительной среды [13, 14]. В настоящее время с ЗОС Горизонт проводятся тематические исследования по требованиям нормативных документов ФСБ России;

– использования в качестве общесистемного программного обеспечения отечественной доверенной операционной системы реального времени ТрастОС КПДА.10966-01 (производитель ООО «СВД Встраиваемые Системы»). В настоящее время с ДОС РВ проводятся тематические исследования по требованиям нормативных документов ФСБ России;

– использования специального программного обеспечения, реализующего фильтрацию и преобразование информации в соответствии с протоколом взаимодействия и прошедшего тематические исследования по требованиям нормативных документов ФСБ России;

– обеспечения встроенными средствами операционной системы функций защиты от несанкционированного доступа и контроля целостности программного обеспечения СДУ АИ.

При этом разработчиком АСЗИ и эксплуатирующей организацией должно быть обеспечено выполнение организационно-режимных и технических мер защиты информации от несанкционированного доступа в АСЗИ [15].

Перед вводом в эксплуатацию СДУ АИ необходимо провести специальный инженерный анализ и расчет специальной надежности. При оценке допустимо руководствоваться методом расчета надежности, который учитывает актуальные для системы угрозы информационной безопасности [16, 17, 18]. При проведении анализа должна быть проверена оценка корректности реализации аппаратно-программного обеспечения устройства, принятого комплекса организационно-технических мер по его эксплуатации, проведены исследования, в том числе экспериментальные, подтверждающие соответствие заявленного алгоритма функционирования СДУ АИ фактическому.

Окончательные выводы о возможности применения СДУ АИ для каждой конкретной АСЗИ делает экспертная организация ФСБ России по результатам экспертизы материалов, отражающих реализацию требований по встраивании СКЗИ в АСЗИ и принятых мер по защите от возникновения угроз информационной безопасности в АСЗИ.

Унифицированная архитектура СДУ АИ, удовлетворяющая всем рассмотренным требованиям, приведена на рис. 3.

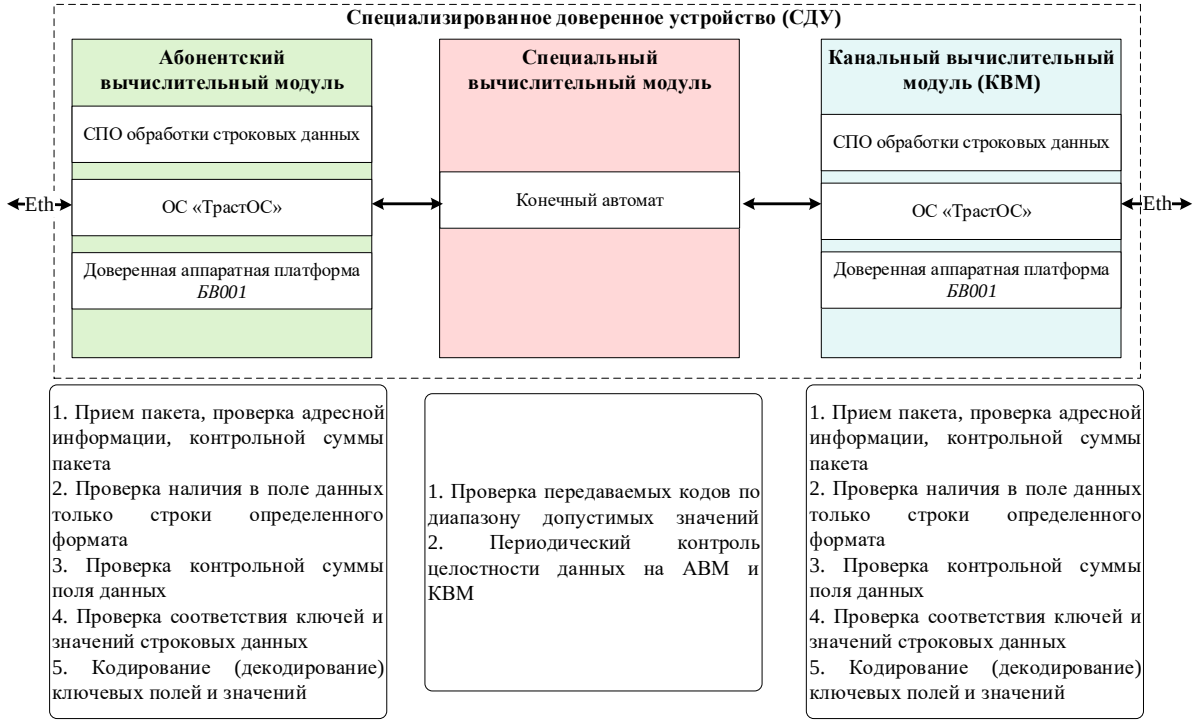


Рис. 3. Унифицированная архитектура СДУ АИ
Fig. 3. Unified architecture of the specialized trusted device for analyzing service information

3. Настройка СДУ АИ и обмен управляющей информацией

С целью возможности применения СДУ АИ в различных АСЗИ, для управления различными типами каналообразующих средств предлагается реализовать на абонентском и канальном вычислительных модулях программное обеспечения работы с базами данных управляющей информации и предусмотреть для данного изделия режим конфигурации. В данном режиме база данных, содержащая определенные по результатам анализа управляющей информации допустимые значения рассмотренного выше протокола взаимодействия, может быть записана на абонентский и канальный вычислительные модули СДУ АИ.

Схема работы СДУ АИ в режиме конфигурации приведена на рис. 4.

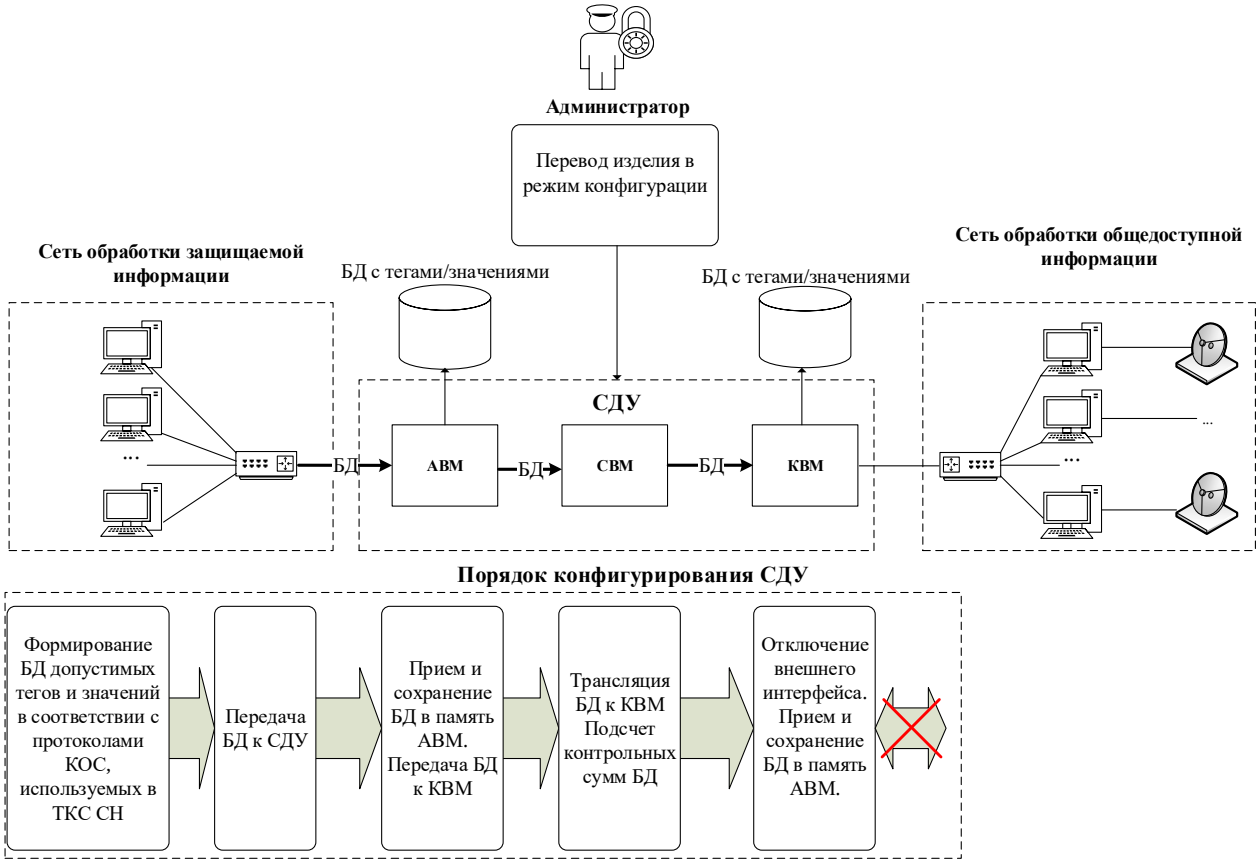


Рис. 4. Порядок конфигурирования СДУ АИ
Fig. 4. Configuration of the specialized trusted device for analyzing service information

Защита от попадания информации ограниченного доступа в каналы связи и от воздействия нарушителя по каналам связи будет обеспечиваться за счет следующих факторов:

– проверка (на АВМ и на КВМ) следующих данных:
  - адресной информации пакета;
  - контрольных сумм;
  - текстового формата и вида «ключ-значение» сообщения;
  - наличия в базе данных всех ключей и значений сообщения.

– преобразование и восстановление ключей и значений сообщения на АВМ и КВМ и невозможность «сквозного» обмена сообщениями между сетями;

– проверка соответствия значений диапазону допустимых значений на СВМ;

– периодический контроль целостности данных специального программного обеспечения и баз данных СДУ АИ;

– комплекс организационно-технических мер защиты информации от несанкционированного доступа, реализованный в АСЗИ.

Описанный порядок обработки управляющей информацией, циркулирующей в АСЗИ через СДУ АИ, приведен на рис. 5.

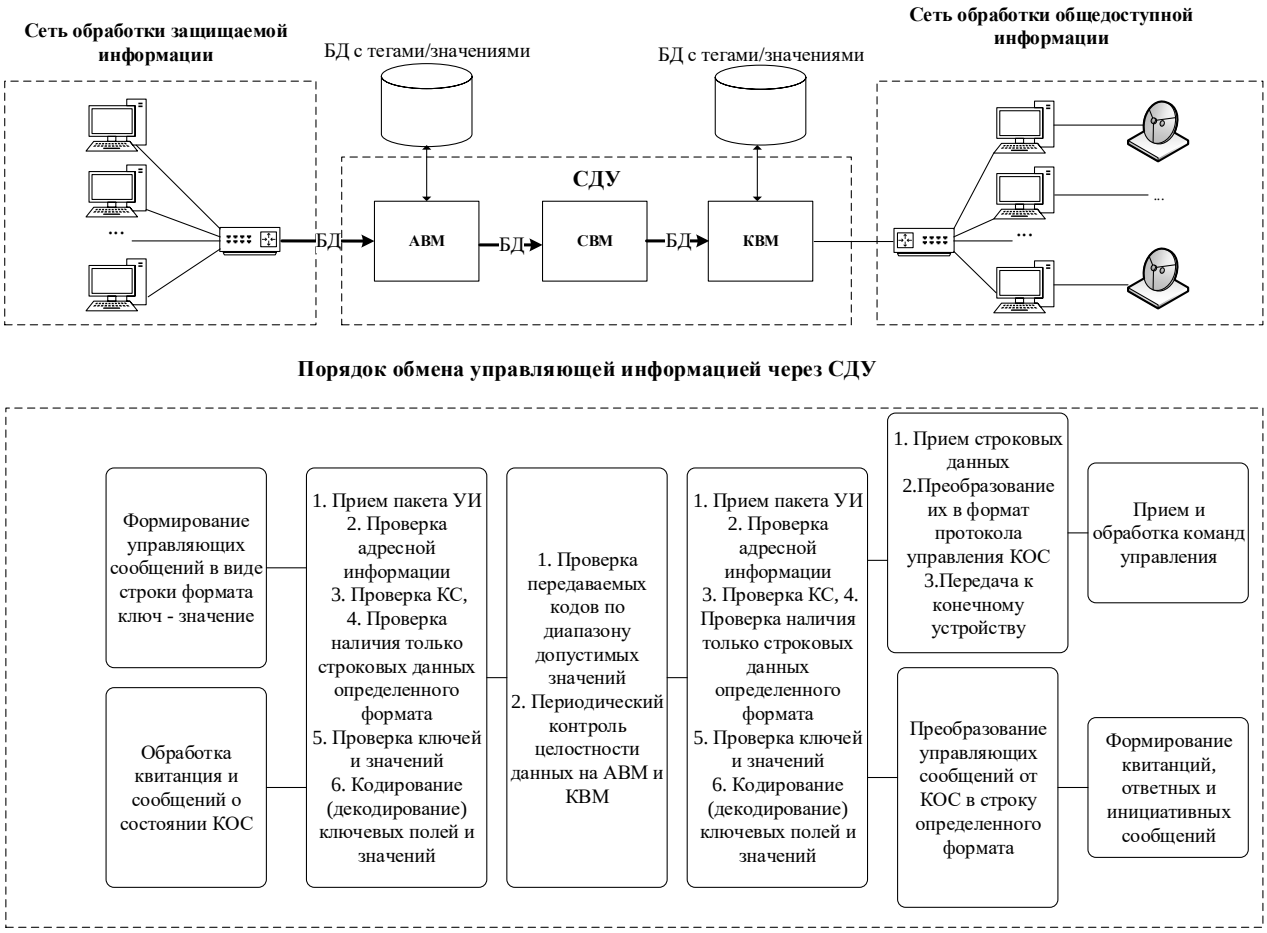


Рис. 5. Порядок обмена управляющей информацией через СДУ АИ
Fig. 5. The procedure for exchanging information through the specialized trusted device for analyzing service information

Таким образом, при условии корректной аппаратно-программной реализации механизмов контроля и фильтрации информации, выполнения комплекса технических мер защиты от несанкционированного доступа к аппаратно-программному обеспечению, а также реализации комплекса организационно-режимных мер при встраивании СДУ АИ в АСЗИ [19, 20], разработанных по результатам проведения специального инженерного анализа по требованиям нормативных документов ФСБ России, СДУ АИ может быть применено в АСЗИ для контроля и фильтрации информации при автоматизированном управлении каналообразующими средствами.

Заключение

В результате проведения работ получен способ создания специализированного доверенного устройства анализа информации на базе доверенной аппаратно-программной платформы. Предложенная архитектура построения СДУ АИ позволяет осуществлять контроль и фильтрацию информации в АСЗИ при управлении каналообразующими средствами и обеспечивает гибкую настройку и минимальную доработку программного обеспечения при встраивании СДУ АИ в конкретную АСЗИ. СДУ АИ обеспечивает защиту от возникновения угроз информационной безопасности при использовании СКЗИ в АСЗИ, в которой реализованы функций автоматизированного управления каналообразующими средствами.

СПИСОК ЛИТЕРАТУРЫ:

1. Чуднов А.М., Путилин А.Н., Попов А.И. Комплексное управление маршрутизацией пакетов и режимами работы радиосредств в неоднородной сети передачи данных. РТС. 2019, № 1 (33), с. 46–56. URL: https://cyberleninka.ru/article/n/kompleksnoe-upravlenie-marshrutizatsiey-paketov-i-rezhimami-raboty-radiosredstv-v-neodnorodnoy-seti-peredachi-dannyh (дата обращения: 16.01.2022).
2. Гутгарц Р.Д., Полякова П.М. Анализ особенностей формулирования функциональных требований к автоматизированной информационной системе. Программные продукты и системы. 2019, № 3, с. 358–367. URL: https://cyberleninka.ru/article/n/analiz-osobennostey-formulirovaniya-funktsionalnyh-trebovaniy-k-avtomatizirovannoy-informatsionnoy-sisteme (дата обращения: 26.02.2022).
3. Бирюков А. Устройства однонаправленной передачи данных. Системный администратор. 2018, № 1–2, с. 182–183. URL: http://samag.ru/archive/article/3579 (дата обращения: 16.01.2022).
4. Воронцов А.Г., Петунин С.А. Организация однонаправленных сетей передачи информации в условиях защищённой среды. Вопросы кибербезопасности. 2017, № 2 (20), с. 21–29. URL: https://cyberleninka.ru/article/n/organizatsiya-odnonapravlennyh-setey-peredachi-informatsii-v-usloviyah-zaschische-nnoy-sredy (дата обращения: 16.01.2022).
5. Авсентьев О.С., Рубцова И.О. Методика оценки аналогии математической модели показателя эффективности защиты информации в компьютерных системах. Вестник ВИ МВД России. 2018, № 2, с. 30–36. URL: https://cyberleninka.ru/article/n/metodika-otsenki-analogii-matematicheskoy-modeli-pokazatelya-effektivnosti-zaschity-informatsii-v-kompyuternyh-sistemah (дата обращения: 26.02.2022).
6. Майер Р.В. Автоматизированный метод оценки количества различных видов информации и ее сложности в физическом тексте с помощью ПЭВМ. Известия ВУЗов. Поволжский регион. Гуманитарные науки. 2014, № 3 (31), с. 200–209. URL: https://cyberleninka.ru/article/n/avtomatizirovannyy-metod-otsenki-kolichestva-razlichnyh-vidov-informatsii-i-ee-slozhnosti-v-fizicheskom-tekste-s-pomoschyu-pevm (дата обращения: 16.01.2022).
7. Беседина К.В. Особенности языка разметки xml. European research. 2016, № 8 (19), с. 51–52. URL: https://cyberleninka.ru/article/n/osobennosti-yazyka-razmetki-xml (дата обращения: 26.02.2022).
8. Шульман В.Д., Шабанов В.В., Сухов П.А., Чунихин А.О. Сравнительный анализ форматов сериализации и передачи данных JSON, XML, CBOR И GPB. StudNet. 2021. № 7, с. 1686–1696. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-formatov-serializatsii-i-peredachi-dannyh-json-xml-cbor-i-gpb (дата обращения: 26.02.2022).
9. Диченко С.А. Контроль и обеспечение целостности информации в системах хранения данных. Наукоемкие технологии в космических исследованиях Земли. 2019. № 1, с. 49–57. URL: https://cyberleninka.ru/article/n/kontrol-i-obespechenie-tselostnosti-informatsii-v-sistemah-hraneniya-dannyh (дата обращения: 26.02.2022).
10. Клименко С.В., Яковлев В.В., Благовещенская Е.А. Исследование реализаций алгоритмов контрольной суммы CRC32. Известия Петербургского университета путей сообщения. 2018, № 3, с. 471–477. URL: https://cyberleninka.ru/article/n/issledovanie-realizatsiy-algoritmov-kontrolnoy-summy-crc32 (дата обращения: 16.01.2022).
11. Боровиков А.Ю., Новиков К.Б., Маслов О.А. Описание подхода программной реализации модуля доверенной загрузки операционной системы. Наукоемкие технологии в космических исследованиях Земли. 2019, № 1, с. 43–48. URL: https://cyberleninka.ru/article/n/opisanie-podhoda-programmnoy-realizatsii-modulya-doverennoy-zagruzki-operatsionnoy-sistemy (дата обращения: 16.01.2022).
12. Боровиков А.Ю., Маслов О.А., Мордвинов С.А., Есафьев А.А. Повышение уровня доверия к аппаратно-программным платформам с целью предупреждения компьютерных атак из-за уязвимостей в ПО BIOS. Вопросы кибербезопасности. 2021, № 6 (46), с. 68–77.

URL: https://cyberleninka.ru/article/n/povyshenie-urovnya-doveriya-k-apparatno-programmnym-platformam-s-tselyu-preduprezhdeniya-kompyuternyh-atak-iz-za-uyazvimostey-v-po (дата обращения: 26.02.2022).
13. Гефнер И.С., Марков А.С. Механизмы реализации атак на уровне базовой системы ввода/вывода. Защита информации. Инсайд. 2017, № 5, с. 80–83. URL: https://www.elibrary.ru/item.asp?id=30268272 (дата обращения: 26.02.2022).
14. Чернов А.Ю., Коноплев А.С. Задача построения доверенной вычислительной среды на аппаратной платформе Intel. Проблемы информационной безопасности. Компьютерные системы. 2016, № 4, с. 36–41. URL: https://jisp.ru/article/zadacha-postroeniya-doverennoj-vychislitelnoj-sredy-na-apparatnoj-platforme-intel/ (дата обращения: 26.02.2022).
15. Авсентьев О.С., Вальде А.Г., Конкин Ю.В. Обеспечение защиты информации в процессе создания информационной системы объекта информатизации. Вестник ВИ МВД России. 2021, № 3, с. 36–48. URL: https://cyberleninka.ru/article/n/obespechenie-zaschity-informatsii-v-protsesse-sozdaniya-informatsionnoy-sistemy-obekta-informatizatsii (дата обращения: 26.02.2022).
16. Беззатеев С.В., Волошина Н.В., Санкин П.С. Методика расчета надежности сложных систем, учитывающая угрозы информационной безопасности. Информационно-управляющие системы. 2014, № 3 (70), с. 78–83. URL: https://cyberleninka.ru/article/n/metodika-rascheta-nadezhnosti-slozhnyh-sistem-uchityvayuschaya-ugrozy-informatsionnoy-bezopasnosti (дата обращения: 16.01.2022).
17. Удалов В.П. Эффективность метода экспертного оценивания модели надежности технической системы безопасности. Вестник ВИ МВД России. 2019, № 2, с. 113–122. URL: https://cyberleninka.ru/article/n/effektivnost-metoda-ekspertnogo-otsenivaniya-modeli-nadezhnosti-tehnicheskoy-sistemy-bezopasnosti (дата обращения: 26.02.2022).
18. Гаранин А.И. О функциональной надежности информационных систем. ИТНОУ: информационные технологии в науке, образовании и управлении. 2018, № 2 (6), с. 45–50. URL: https://cyberleninka.ru/article/n/o-funktsionalnoy-nadezhnosti-informatsionnyh-sistem (дата обращения: 26.02.2022).
19. Родионов А.С., Белянин В.И., Горбунов А.А. Совершенствование методов защиты информации от несанкционированного доступа. NBI-technologies. 2018, № 2, с. 39–43. URL: https://cyberleninka.ru/article/n/sovershenstvovanie-metodov-zaschity-informatsii-ot-nesanktsionirovannogo-dostupa (дата обращения: 26.02.2022).
20. Качаева Г.И., Попов А.Д., Рогозин Е.А. Показатели эффективности функционирования при разработке систем защиты информации от несанкционированного доступа в автоматизированных информационных системах. Вестник ДГТУ. Технические науки. 2018, № 1, с. 147–149. URL: https://cyberleninka.ru/article/n/pokazateli-effektivnosti-funktsionirovaniya-pri-razrabotke-sistem-zaschity-informatsii-ot-nesanktsionirovannogo-dostupa-v (дата обращения: 26.02.2022).

REFERENCES:

[1] Chudnov A.M., Putilin A.N., Popov A.I. Kompleksnoe upravlenie marshrutizaciej paketov i rezhimami raboty radiosredstv v neodnorodnoj seti peredachi dannyh. RTS. 2019, № 1 (33). URL: https://cyberleninka.ru/article/n/kompleksnoe-upravlenie-marshrutizatsiey-paketov-i-rezhimami-raboty-radiosredstv-v-neodnorodnoy-seti-peredachi-dannyh (accessed: 16.01.2022) (in Russian).
[2] Gutgarts R.D., Polyakova P.M. Analysis of the features of the formulation of functional requirements for an automated information system. Software products and systems. 2019, no. 3, p. 358–367. URL: https://cyberleninka.ru/article/n/analiz-osobennostey-formulirovaniya-funktsionalnyh-trebovaniy-k-avtomatizirovannoy-informatsionnoy-sisteme (accessed: 26.02.2022) (in Russian).
[3] Biryukov A. Ustrojstva odnonapravlennoj peredachi dannyh. Sistemnyj administrator. 2018, № 1–2, s. 182–183. URL: http://samag.ru/archive/article/3579 (accessed: 16.01.2022) (in Russian).
[4] Voroncov A.G., Petunin S.A. Organizaciya odnonapravlennyh setej peredachi informacii v usloviyah zashchishchënnoj sredy. Voprosy kiberbezopasnosti. 2017, № 2 (20), s. 21–29. URL: https://cyberleninka.ru/article/n/organizatsiya-odnonapravlennyh-setey-peredachi-informatsii-v-usloviyah-zaschische-nnoy-sredy (accessed: 16.01.2022) (in Russian).
[5] Avsentiev O.S., Rubtsova I.O. Methods for evaluating the analogy of the mathematical model of the indicator of the effectiveness of information protection in computer systems. Bulletin of the VI Ministry of Internal Affairs of Russia. 2018, no. 2, p. 30–36. URL: https://cyberleninka.ru/article/n/metodika-otsenki-analogii-matematicheskoy-modeli-pokazatelya-effektivnosti-zaschity-informatsii-v-kompyuternyh-sistemah (accessed: 26.02.2022) (in Russian).
[6] Majer R.V. Avtomatizirovannyj metod ocenki kolichestva razlichnyh vidov informacii i ee slozhnosti v fizicheskom tekste s pomoshch'yu PEVM. Izvestiya VUZov. Povolzhskij region. Gumanitarnye nauki. 2014, № 3 (31), s. 200-209. URL: https://cyberleninka.ru/article/n/avtomatizirovannyy-metod-otsenki-kolichestva-razlichnyh-vidov-informatsii-i-ee-slozhnosti-v-fizicheskom-tekste-s-pomoschyu-pevm (accessed: 16.01.2022) (in Russian).

[7] Besedina K.V. Osobennosti yazyka razmetki xml. European research. 2016, № 8 (19), s. 51–52. URL: https://cyberleninka.ru/article/n/osobennosti-yazyka-razmetki-xml (accessed: 16.01.2022) (in Russian).
[8] Shulman V.D., Shabanov V.V., Sukhov P.A., Chunikhin A.O. Comparative analysis of serialization and data transmission formats JSON, XML, CBOR and GPB. StudNet. 2021, no. 7, p. 1686–1696. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-formatov-serializatsii-i-peredachi-dannyh-json-xml-cbor-i-gpb (accessed: 26.02.2022) (in Russian).
[9] Dichenko S.A. Monitoring and ensuring the integrity of information in data storage systems. Science-intensive technologies in space research of the Earth. 2019, no. 1, p. 49–57. URL: https://cyberleninka.ru/article/n/kontrol-i-obespechenie-tselostnosti-informatsii-v-sistemah-hraneniya-dannyh (accessed: 26.02.2022) (in Russian).
[10] Klimenko S.V., YAkovlev V.V., Blagoveshchenskaya E.A. Issledovanie realizacij algoritmov kontrol'noj summy CRC32. Izvestiya Peterburgskogo universiteta putej soobshcheniya. 2018, № 3, s. 471–477. URL: https://cyberleninka.ru/article/n/issledovanie-realizatsiy-algoritmov-kontrolnoy-summy-crc32 (accessed: 16.01.2022) (in Russian).
[11] Borovikov A.Y., Novikov K.B., Maslov O.A. Opisanie podhoda programmnoj realizacii modulya doverennoj zagruzki operacionnoj sistemy. Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. 2019, № 1, s. 43–48. URL: https://cyberleninka.ru/article/n/opisanie-podhoda-programmnoy-realizatsii-modulya-doverennoy-zagruzki-operatsionnoy-sistemy (accessed: 16.01.2022) (in Russian).
[12] Borovikov A.Y., Maslov O.A., Mordvinov S.A., Esafiev A.A. Increasing the level of trust in hardware and software platforms in order to prevent computer attacks due to vulnerabilities in BIOS software. Cybersecurity Issues. 2021, no. 6 (46), p. 68–77. URL: https://cyberleninka.ru/article/n/povyshenie-urovnya-doveriya-k-apparatno-programmnym-platformam-s-tselyu-preduprezhdeniya-kompyuternyh-atak-iz-za-uyazvimostey-v-po (accessed: 26.02.2022) (in Russian).
[13] Gefner I.S., Markov A.S. Mechanisms for Implementing Attacks at the Level of the Basic Input/Output System. Information Security. Inside. 2017, no. 5, p. 80–83. URL: https://www.elibrary.ru/item.asp?id=30268272 (accessed: 26.02.2022) (in Russian).
[14] Chernov A.Yu., Konoplev A.S. The task of building a trusted computing environment on the Intel hardware platform. Problems of information security. Computer systems. 2016, no. 4, p. 36–41. URL: https://jisp.ru/article/zadacha-postroeniya-doverennoj-vychislitelnoj-sredy-na-apparatnoj-platforme-intel/ (accessed: 26.02.2022) (in Russian).
[15] Avsentiev O.S., Valde A.G., Konkin Yu.V. Ensuring the protection of information in the process of creating an information system of an informatization object. Bulletin of the VI Ministry of Internal Affairs of Russia. 2021, no. 3, p. 36–48. URL: https://cyberleninka.ru/article/n/obespechenie-zaschity-informatsii-v-protsesse-sozdaniya-informatsionnoy-sistemy-obekta-informatizatsii (accessed: 26.02.2022) (in Russian).
[16] Bezzateev S.V., Voloshina N.V., Sankin P.S. Metodika rascheta nadezhnosti slozhnyh sistem, uchityvayushchaya ugrozy informacionnoj bezopasnosti. Informacionno-upravlyayushchie sistemy. 2014, № 3 (70), s. 78–83. URL: https://cyberleninka.ru/article/n/metodika-rascheta-nadezhnosti-slozhnyh-sistem-uchityvayuschaya-ugrozy-informatsionnoy-bezopasnosti (accessed: 16.01.2022) (in Russian).
[17] Udalov V.P. Efficiency of the method of expert evaluation of the reliability model of a technical security system. Bulletin of the VI Ministry of Internal Affairs of Russia. 2019, no. 2, p. 113–122. URL: https://cyberleninka.ru/article/n/effektivnost-metoda-ekspertnogo-otsenivaniya-modeli-nadezhnosti-tehnicheskoy-sistemy-bezopasnosti (accessed: 26.02.2022) (in Russian).
[18] Garanin A.I. On the functional reliability of information systems. ITNOU: information technologies in science, education and management. 2018, no. 2 (6), p. 45–50. URL: https://cyberleninka.ru/article/n/o-funktsionalnoy-nadezhnosti-informatsionnyh-sistem (accessed: 26.02.2022) (in Russian).
[19] Rodionov A.S., Belyanin V.I., Gorbunov A.A. Improving methods of protecting information from unauthorized access. NBI-technologies. 2018, no. 2, p. 39–43. URL: https://cyberleninka.ru/article/n/sovershenstvovanie-metodov-zaschity-informatsii-ot-nesanktsionirovannogo-dostupa (accessed: 26.02.2022) (in Russian).
[20] Kachaeva G.I., Popov A.D., Rogozin E.A. Performance indicators in the development of information protection systems from unauthorized access in automated information systems. Bulletin of the DSTU. Technical science. 2018, no. 1, p. 147–149. URL: https://cyberleninka.ru/article/n/pokazateli-effektivnosti-funktsionirovaniya-pri-razrabotke-sistem-zaschity-informatsii-ot-nesanktsionirovannogo-dostupa-v (accessed: 26.02.2022) (in Russian).

Поступила в редакцию - 18 октября 2021 г. Окончательный вариант – 28 февраля 2022 г.
Received – October 18, 2021. The final version – February 28, 2022.

Сергей В. Запечников
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
e-mail: SVZapechnikov@mephi.ru, http://orcid.org/0000-0002-7975-6040

КОНФИДЕНЦИАЛЬНОЕ МАШИННОЕ ОБУЧЕНИЕ НА ОСНОВЕ ТРЕХСТОРОННИХ ПРОТОКОЛОВ БЕЗОПАСНЫХ ВЫЧИСЛЕНИЙ*

DOI: http://dx.doi.org/10.26583/bit.2022.1.04

Аннотация. Статья посвящена анализу систем конфиденциального машинного обучения, основанных на концепции безопасных трехсторонних вычислений. После общих сведений о постановках задач безопасных многосторонних вычислений и конфиденциального машинного обучения проводится обзор существующих систем конфиденциального машинного обучения и перспектив их развития. Анализ работ ведущих зарубежных исследовательских коллективов позволяет выделить ряд критериев, существенных для оценки систем конфиденциального машинного обучения на основе многосторонних протоколов безопасных вычислений. Проводится сравнительная оценка систем конфиденциального машинного обучения по выделенной системе критериев. Дальнейшим предметом рассмотрения являются только системы на основе трехсторонних протоколов безопасных вычислений. Основное внимание уделяется алгоритмическим аспектам организации таких систем, реализованных в них методам и протоколам защиты информации. Рассматриваются системы, стойкие к различным типам противника, как основанные на универсальных модулях безопасных двусторонних вычислений, так и специализированные, предназначенные для обеспечения конфиденциальности конкретных методов машинного обучения, таких как нейронные сети. Подробно рассматриваются примеры прототипов таких систем. Основываясь на результатах проведенного анализа, формулируются выводы о перспективах развития систем конфиденциального машинного обучения, ставятся задачи продолжения исследований.

Ключевые слова: конфиденциальное машинное обучение, безопасные многосторонние вычисления, схемы разделения секрета, гомоморфное шифрование.

Для цитирования: ЗАПЕЧНИКОВ, Сергей В. КОНФИДЕНЦИАЛЬНОЕ МАШИННОЕ ОБУЧЕНИЕ НА ОСНОВЕ ТРЕХСТОРОННИХ ПРОТОКОЛОВ БЕЗОПАСНЫХ ВЫЧИСЛЕНИЙ. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 30–43, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1400. DOI: http://dx.doi.org/10.26583/bit.2022.1.04.

***Благодарности.** Работа выполнена при поддержке Министерства науки и высшего образования РФ (проект государственного задания № 0723-2020-0036).*

Sergey V. Zapechnikov
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: SVZapechnikov@mephi.ru, http://orcid.org/0000-0002-7975-6040

Privacy-preserving machine learning based on secure three-party computations*

DOI: http://dx.doi.org/10.26583/bit.2022.1.04

Abstract. The paper is devoted to the analysis of privacy-preserving machine learning systems based on the concept of secure three-party computations. After general information about the purposes of secure multi-party computations and privacy-preserving machine learning, an overview of existing privacy-preserving machine learning systems and perspectives for their development is offered. An analysis of the work of leading foreign research teams allows to identify several criteria essential for evaluating privacy-preserving machine learning systems based on multi-party secure computations. A comparative analysis of privacy-preserving machine learning systems is carried out according to a dedicated system of criteria. The further

subject of consideration is only systems based on three-party secure computations. The main attention is paid to the algorithmic aspects of the organization of such systems, the methods and protocols of information security implemented in them. Systems secure to various types of adversary are considered, both based on universal modules of secure two-party computations, and specialized ones designed to ensure the privacy of specific machine learning methods, such as neural networks. Examples of prototypes of such systems are considered in detail. Based on the results of the analysis, conclusions are made about the prospects for developing privacy-preserving machine learning systems, and the tasks of future research are described.

Keywords: privacy-preserving machine learning, secure multi-party computations, secret sharing scheme, homomorphic encryption.

For citation: ZAPECHNIKOV, Sergey V. Privacy-preserving machine learning based on secure three-party computations. IT Security (Russia), [S.l.], v. 29, n. 1, p. 30–43, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1400. DOI: http://dx.doi.org/10.26583/bit.2022.1.04.

***Acknowledgement.** This work was supported by the Ministry of Science and Higher Education of the Russian Federation (state assignment project No. 0723-2020-0036).*

Введение

Безопасные многосторонние вычисления (БМВ) – одно из важнейших направлений развития современной криптографии. Напомним постановку задачи БМВ [1]. Рассматривается многосторонний криптографический протокол, в котором каждый из участников имеет свой индивидуальный секрет. Требуется вычислить заданную функцию, аргументами которой являются эти секреты, так чтобы результат вычислений был известен всем участникам группы, но сами секреты не были разглашены участниками протокола ни друг другу, ни какой-либо третьей стороне. А именно, пусть участники криптографического протокола $P_1, P_2, \dots, P_n$ имеют конфиденциальные входные данные $x_1, x_2, \dots, x_n$ соответственно. В результате выполнения протокола ими совместно должна быть вычислена функция вида $y = f(x_1, x_2, \dots, x_n)$, при этом протокол должен обладать следующими двумя свойствами:

- *корректностью*: каждый из участников $P_1, P_2, \dots, P_n$ получает y;
- *приватностью* (конфиденциальностью): никому из участников либо третьих лиц не разглашается никакая дополнительная информация, кроме той, которую они знали до начала выполнения протокола.

Частным случаем БМВ можно считать задачу конфиденциального машинного обучения (КМО). Целью КМО является обеспечение конфиденциальности данных каждого из участников системы машинного обучения в условиях, когда лица, предоставляющие обучающую выборку на этапе обучения модели (training) либо запросы к модели на этапе ее эксплуатации (inference) и ожидающие получения ответов на свои запросы (клиенты), дистанционно взаимодействуют с провайдером, способным выполнять вычисления с помощью этой модели (сервером). Задача КМО может решаться при помощи БМВ с разным числом участников. Настоящая статья посвящена преимущественно исследованию случая, когда КМО реализуется на основе трехсторонних протоколов безопасных вычислений, т.е. в приведенной выше постановке задачи n=3.

Предлагаемая вниманию читателя статья является продолжением исследования, посвященного КМО на основе двусторонних протоколов безопасных вычислений [2].

1. Системы КМО и перспективы их развития

Как показывает анализ научной литературы, в настоящее время теоретические и прикладные исследования в сфере разработки и реализации систем КМО выполняет не менее 10 научных коллективов, рассредоточенных по всему миру. В связи с высоким

темпом научных исследований в области систем КМО рассматривались только системы, созданные за последние три года (2019–2021 гг.). Далее приведем краткие сведения о работах каждого из коллективов.

1. *Коллектив международного исследовательского подразделения корпорации Microsoft*. Усилия коллектива сосредоточены на создании систем КМО двухуровневой архитектуры, в которых клиентские компоненты позволяют интерпретировать описания моделей машинного обучения, выполненные с помощью средств библиотеки TensorFlow во внутреннее представление, а серверные компоненты – автоматически исполнять протоколы БМВ, реализующие вычисления, при помощи модулей с набором универсальных двухсторонних и трехсторонних протоколов безопасных вычислений.

Основные работы коллектива:

- система SecureNN (2019 г.) [3];
- система EzPC (2019 г.) [4];
- система CrypTFlow (2020 г.) [5];
- система CrypTFlow2 (inference, 2020) [6].

2. *Исследовательская группа Дармштадтского технического университета* (ФРГ). Основное направление работы коллектива в области систем КМО – реализация универсальных средств исполнения двусторонних протоколов безопасных вычислений на основе сочетания представления вычисляемых функций в виде арифметических, булевых и искаженных схем (garbled circuits), которые могут использоваться в виде готового ядра при создании отдельных приложений, включая федеративное обучение, обработку медицинских изображений методами машинного обучения и пр.

Основные работы коллектива:

- модуль ABY (2015 г.) [7];
- система MP2ML (2020 г.) [8];
- модуль ABY 2.0 (2020 г.) [9];
- система FLGuard (2021 г.) [10].

3. *Исследовательская группа Калифорнийского университета в Беркли* (UC Berkeley, США). Коллектив работает в области создания систем КМО для получения ответов на запросы, содержащие конфиденциальную информацию, к уже обученным моделям на основе двусторонних протоколов безопасных вычислений с усиленными свойствами, включая самую «сильную» модель нарушителя – модель злоумышленного клиента.

Основные работы коллектива:

- система Delphi (2018 г.) [11];
- экспериментальные системы и прототипы Visor, Bost, Cerebro (2019–2021 гг.) [12];
- система Muse (2021 г.) [13].

4. *Исследовательская группа Индийского института наук в Бангалоре* (Indian Institute of Science, Bangalor). Деятельность научной группы сосредоточена на создании систем КМО преимущественно для глубоких нейронных сетей на основе четырехсторонних протоколов безопасных вычислений с возможностью реализации некоторых систем и на трехсторонних протоколах.

Основные работы коллектива:

- Trident (2020 г.) [14];
- FLASH (2020 г.) [15];
- Blaze (2020 г.) [16];

- SWIFT (2021 г.) [17];
- Tetrad (2021 г.) [18].

Совместно с Дармштадтским университетом члены исследовательской группы участвовали в разработке модуля ABY 2.0 [9].

5. *Группа исследователей из компании Facebook и Visa Research*. Деятельность членов команды сосредоточена на создании универсального модуля для трехсторонних протоколов безопасных вычислений на основе сочетания арифметических, булевых и искаженных схем, а также создания прикладных систем КМО на его основе. В настоящее время основное внимание уделяется протоколам и системам конфиденциальной кластеризации.

Основные работы коллектива:

- SecureML (2017 г.) [19];
- ABY^3 (Arithmetic-Binary-Yao) framework (2018 г.) [20];
- K-means clustering (2020 г.) [21].

6. *Исследовательская группа Принстонского университета* (США) занимается разработкой систем КМО на основе трехсторонних протоколов безопасных вычислений со все более строгими моделями нарушителей.

Основные работы коллектива:

- SecureNN (2019 г., совместно с Microsoft) [3];
- FALCON (2021 г.) [22];
- Ponytail (2012–2021 гг.) [23].

7. *Международная исследовательская группа Национального института индустриальных наук и технологий Японии, корпорации NTT и университета Санкт-Галлен* (Швейцария). Имеются сведения об одной разработке этого коллектива – системе КМО Adam для глубоких нейросетей, поддерживающая расширенную по сравнению с известными функциональность при обучении и применении нейросетей [24]. Система основана на трехсторонних протоколах безопасных вычислений.

8. *Исследовательская группа Массачусетского технологического института* (США). Имеются сведения об одной разработке этой группы – системе Gazelle (2018 г.) [25] на основе двусторонних протоколов. В настоящее время отдельные идеи этой разработки используются в более новых системах КМО, а сама система Gazelle представляет исторический интерес.

9. *Исследовательская группа университета Аальто* (Финляндия). Имеются сведения об одной разработке этой группы – системе MiniONN (2017 г.) [26], которая представляет лишь исторический интерес, поскольку уступает более новым системам КМО по всем основным показателям.

10. Исследовательская группа Парижского университета (Франция). Имеются сведения об одной разработке этой группы – системе AriaNN [27], которая также представляет лишь исторический интерес, поскольку уступает более новым системам КМО по всем основным показателям.

2. Критерии оценки систем КМО

Анализ работ исследовательских коллективов позволяет выделить ряд критериев, существенных для оценки разработанных и реализованных систем КМО на основе протоколов БМВ. Далее охарактеризуем их подробнее.

1. *Количество сторон в протоколах БМВ*, реализующих функциональность систем КМО:

1.1) двусторонние;

1.2) трехсторонние;

1.3) четырехсторонние.

Некоторые системы КМО позволяют реализовывать функциональность посредством протоколов с разным числом участников. В то же время систем с количеством участников вычислений более четырех в ходе настоящего исследования обнаружено не было.

2. *Криптографические примитивы*, используемые для реализации системы:

2.1) схемы разделения секрета;

2.2) искаженные схемы (garbled circuits);

2.3) схемы гомоморфного шифрования.

Для большинства систем характерно сочетание двух или даже всех трех перечисленных типов криптографических примитивов, хотя есть попытки построить системы КМО, используя только один вид примитивов, но они, как правило, обладают ограниченной функциональностью.

3. *Модель нарушителя*, в предположении о которой разрабатывалась система КМО и в которой обеспечивается ее криптографическая стойкость:

3.1) получестный нарушитель;

3.2) злоумышленный нарушитель.

Подавляющее большинство систем, основанных на двусторонних протоколах безопасных вычислений, обеспечивают стойкость к получестному нарушителю, в то время как абсолютное большинство систем, основанных на трех- и четырехсторонних протоколах обеспечивает стойкость как к получестному, так и к злоумышленному нарушителю.

4. *Поддержка стадий жизненного цикла машинного обучения*:

4.1) обучение моделей (training);

4.2) применение моделей для получения прогнозных ответов на запросы пользователей (inference).

Стадия обучения моделей является многократно (иногда на несколько порядков величины) более трудоемкой, чем их применение. В то же время обучение модели – относительно нечасто выполняемая операция по сравнению с последующим применением обученной модели. Как показывает анализ литературы, большая часть систем КМО в настоящее время поддерживает лишь стадию применения уже обученных моделей, в то же время ряд систем поддерживают обе стадии.

5. *Поддержка методов машинного обучения*:

5.1) элементарных статистических и логических методов машинного обучения (линейная регрессия, логистическая регрессия, кластеризация, решающие деревья);

5.2) полносвязных нейронных сетей;

5.3) глубоких нейронных сетей;

5.4) специальных приемов обучения и применения нейронных сетей для повышения точности прогнозирования, производительности, сходимости параметров сети и т.п., таких как пакетная нормализация, оптимизация по методу Adam и др.

Как показывает анализ, среди систем КМО преобладают разработки для обеспечения безопасности глубоких нейронных сетей, прежде всего, сверточных. Нарастает количество работ, посвященных обеспечению конфиденциальности при использовании специальных приемов обучения нейросетей, часто используемых на практике.

6. *Пригодность для использования в различных коммуникационных архитектурах*:

6.1) локальных компьютерных сетях (LAN);

6.2) глобальных компьютерных сетях (WAN).

Системы КМО, которые реализуются посредством протоколов БМВ с большой коммуникационной сложностью, а также со сбалансированными требованиями к

коммуникационным и вычислительным ресурсам участников значительно лучше подходят для локальных сетей. В то же время системы КМО, предназначенные для глобальных сетей, должны минимизировать коммуникационные требования к участникам за счет более высоких вычислительных требований.

7. *Объем массивов данных*, использованных для апробации систем КМО:

7.1) массивы данных относительно малого объема;

7.2) «большие данные».

Многие системы КМО, которые показывают хорошие результаты при экспериментах на относительно малых массивах данных (например, датасет MNIST, часто используемый в качестве эталона для апробации алгоритмов классификации), могут оказаться непрактичными из-за неприемлемо большого времени работы на массивах, представляющих практический интерес. В связи с этим большое значение имеет апробация экспериментальных систем КМО на массивах данных объема, сопоставимого с тем, который будет встречаться при практическом использовании (например, таких как известный эталон CIFAR-10).

8. *Архитектуры нейросетей*, для которых апробированы системы КМО:

8.1) относительно простые нейросети с небольшим количеством слоев (например, LeNet, AlexNet и т.п.);

8.2) глубокие нейросети с числом слоев порядка 50–200 (например, VGG-16, ResNet, DenseNet).

Практический интерес представляют такие системы КМО, которые могут эффективно работать с глубокими нейросетями, получившими наибольшее практическое применение.

3. Сравнительная оценка систем КМО на основе многосторонних протоколов безопасных вычислений

Проанализированные в ходе настоящего исследования системы КМО могут быть охарактеризованы по критериям, перечисленным в предыдущем разделе. Результаты оценки приведены в табл. 1.

Таблица 1. Результаты сравнительной оценки систем КМО

№ п/п	Системы КМО	Критерии оценки																			
		1			2			3		4		5				6		7		8	
		1.1	1.2	1.3	2.1	2.2	2.3	3.1	3.2	4.1	4.2	5.1	5.2	5.3	5.4	6.1	6.2	7.1	7.2	8.1	8.2
1	SecureNN		+	+/-	+			+	+/-	+	+		+	+	+/-	+	+	+		+	
2	EzPC	+			+	+		+			+	+	+			+	+	+	+	+	
3	CrypTFlow	+	+		+			+	+		+			+		+		+	+	+	+
4	CrypTFlow2	+			+			+			+			+		+		+	+	+	+
5	ABY	+			+	+		+		+	+	+				+		+		+	
6	Delphi	+			+	+	+	+			+		+			+		+	+	+	+/-
7	Muse	+			+	+	+	+	+		+		+			+		+	+	+	
8	Trident			+	+	+		+	+	+	+		+			+	+	+		+	
9	FLASH			+	+			+	+		+		+	+		+	+	+	+/-	+	
10	Blaze		+		+	+		+	+	+/-	+	+	+			+	+	+		+	
11	Tetrad			+	+	+		+	+	+	+		+			+	+	+	+	+	+/-
12	SecureML	+			+	+	+	+		+	+	+	+			+	+/-	+		+	
13	ABY[3]		+		+	+		+	+	+	+	+				+	+/-	+		+	
14	Falcon		+		+			+	+	+	+		+	+	+	+	+	+	+	+	+
15	Gazelle	+			+	+	+	+			+		+			+		+	+	+	
16	MiniONN	+			+	+	+	+			+	+	+			+		+	+	+	
17	Система [24]		+		+			+	+	+	+			+	+	+	+	+	+	+	+

Нумерация критериев оценки соответствует введенной в п. 2 настоящей статьи. Условные обозначения: «+» – соответствие критерию (наличие свойства), «-» – несоответствие критерию (отсутствие свойства), «+/-» – частичное соответствие критерию (наличие части свойств).

Эти результаты свидетельствуют о том, что в качестве основного классификационного признака систем КМО целесообразно использовать количество сторон в протоколах БМВ, реализующих функциональность систем КМО. Этот признак позволяет вполне определенно разделить все системы на три класса – системы, основанные на двусторонних, трехсторонних и четырехсторонних протоколах.

Дальнейшим предметом рассмотрения в настоящей статье являются системы КМО на основе трехсторонних протоколов безопасных вычислений.

4. Системы КМО на основе трехсторонних протоколов безопасных вычислений

Основное внимание будем уделять алгоритмическим аспектам организации систем, а также методам и протоколам защиты данных в них.

Модуль ABY³. Модуль ABY^3 [20] задуман и реализован как виртуальный процессор, выполняющий набор базовых операций для трехсторонних протоколов безопасных вычислений над целыми числами. Основная идея заключается в использовании трех форм разделения секрета: арифметического, булева и Яо-разделения, вычислений с использованием соответствующих схем и переключений между ними для выбора наиболее производительного протокола вычислений. Модуль реализован на языке C++. Среди участников протокола допускается наличие не более одного нарушителя: получестного либо злоумышленного.

Внешне идеи модуля ABY^3 выглядят аналогично идеям, заложенным в основу модуля ABY [9], рассмотренного в [2], однако криптографические протоколы сильно отличаются в связи с тем, что разделение секрета здесь трехстороннее.

Для арифметического разделения секретного числа $x \in \mathbb{Z}_{2^k}$ (здесь принято, что k=64) между тремя участниками выбирается три случайных числа $x_1, x_2, x_3 \in \mathbb{Z}_{2^k}$ таких, что $x = x_1 + x_2 + x_3$. Доли секрета распределяются между участниками парами: $\{(x_1, x_2), (x_2, x_3), (x_3, x_1)\}$, где i-й участник протокола хранит i-ю пару долей секрета.

Определяется ряд базовых операций над разделенными секретами: сложение, умножение, разделения на доли нулевого секрета, разделения на доли случайного секрета, сборка секрета из долей, разделение секрета на доли.

Булево разделение секрета определяется как частный случай арифметического при k=1, а вместо операций сложения, вычитания и умножения используются операции $\oplus, \wedge$.

Наиболее оригинальной частью модуля ABY^3 можно считать специальную трехстороннюю схему Яо-разделения секрета для использования в трехстороннем варианте искаженной схемы [28].

Модуль ABY^3 поддерживает следующий набор трехсторонних протоколов безопасных вычислений:

- умножение целых чисел с фиксированной запятой: $z = xy$, где $x, y \in \mathbb{Z}_{2^k}$;
- скалярное умножение двух векторов целых чисел с фиксированной запятой: $\vec{z} = \vec{x} \cdot \vec{y} = \sum_{i=1}^{n} x_i y_i$, где $x, y \in \left(\mathbb{Z}_{2^k}\right)^n$;
- конвертирование долей между различными формами разделения: арифметической, булевой, Яо-разделением;
- умножение разделенного целого числа на разделенный бит;

- вычисление кусочно-полиномиальной функции: пусть $f_1, \dots, f_m$ – многочлены с общеизвестными коэффициентами, и $-\infty = c_0 < c_1 < \cdots < c_{m-1} < c_m = \infty$, такие что

$$f(x) = \begin{cases} f_1(x), x < c_1 \\ f_2(x), c_1 \le x < c_2 \\ \dots\dots\dots \\ f_m(x), c_{m-1} \le x \end{cases},$$

– протокол позволяет вычислить функцию $f(x) = \sum_i b_i f_i(x)$, где $b_1, \dots, b_m \in \{0,1\}$ – вектор разделенных секретных битов таких, что $b_i = 1$ тогда и только тогда, когда $c_{i-1} < x \le c_i$.

Авторы апробировали модуль ABY[3] для обучения и применения линейной регрессии, логистической регрессии, полносвязной трехслойной нейронной сети с функциями активации ReLU, а также сверточной нейронной сети с двумя слоями свертки. При применении обученной сети авторами получено приемлемое время вычислений (6–10 мс) и объем передаваемых данных (порядка 5 МБ). Следует, однако, отметить, что нейросети и датасеты, на которых проводились эксперименты, слишком упрощены по сравнению с моделями, представляющими практический интерес. Исследование влияния протоколов на точность предсказаний моделей не проводилось.

Система CrypTFlow. CrypTFlow представляет собой систему КМО, предназначенную для использования на стадии применения обученных моделей для получения прогнозных ответов на запросы пользователей [5]. Она конвертирует исходный код модели, описанный программистом на языке библиотеки TensorFlow в протоколы БМВ без необходимости для программиста вникать в детали криптографических конструкций.

Архитектура системы CrypTFlow – двухуровневая и включает в себя три компонента. Компонент уровня фронтенд – модуль Athos, который транслирует код библиотеки TensorFlow во внутреннее представление системы. Компоненты уровня бэкенд – модули Porthos и Aramis, которые транслируют функции, записанные модулем Athos на языке внутреннего представления системы CrypTFlow, в протоколы БМВ, стойкие в модели получестного нарушителя.

Модуль Porthos обеспечивает сборку из криптографических примитивов трехстороннего протокола безопасных вычислений. Встроенные в модуль примитивы реализуют функциональность линейных и нелинейных слоев сверточных нейронных сетей. К первому типу относится слой свертки, для чего используется трехсторонний протокол умножения матриц. Ко второму типу относятся функции активации ReLU и Maxpool, для чего используются протоколы безопасного вычисления старшего бита целого числа и конвертации долей секрета.

Модуль Aramis конвертирует любой протокол БМВ, стойкий в модели получестного нарушителя, в протокол, стойкий к злоумышленному нарушителю, с использованием аппаратных функций защиты, которые обеспечиваются процессором. Созданная авторами системы CrypTFlow реализация опирается на функции Intel SGX, однако возможно использование аналогичных функций других процессорных архитектур, например, ARM TrustZone.

В качестве бэкенда может также использоваться модуль ABY [7], который обеспечивает сборку двустороннего протокола безопасных вычислений, реализующего функциональность, описанную на языке внутреннего представления модулем Athos.

Экспериментально продемонстрирована работоспособность системы CrypTFlow на сверточных сетях ResNet50 и DenseNet121 на тестовом датасете ImageNet. Среднее время получения клиентом ответа на свой запрос составило около 30 с при использовании модулей, обеспечивающих стойкость в модели получестного нарушителя, и около 2 мин – в модели злоумышленного нарушителя. Суммарный объем передаваемых в протоколе данных около 7–10 ГБ.

Таким образом, система CrypTFlow может считаться вполне практичной по критериям времени выполнения и точности прогнозирования при двусторонних и трехсторонних вычислениях прогнозных ответов на запросы пользователей по обученной нейросети.

Система SecureNN. SecureNN – это система КМО, поддерживающая трех- и четырехсторонние вычисления при обучении и применении глубоких нейронных сетей [3]. Криптографическая стойкость обеспечивается в модели получестного противника.

В основе системы лежат новые протоколы безопасных вычислений для различных блоков нейросетей:

- умножения матриц;
- вычисления функции ReLU (rectified linear units);
- пулинга по максимальному значению (maxpool);
- пакетной нормализации.

Эти блоки позволяют конструировать трех- и четырехсторонние протоколы, стойкие в теоретико-информационном смысле, для обучения и предсказаний с использованием глубоких нейросетей, в том числе сверточных. Ни одна из сторон протокола не имеет полного доступа к обрабатываемым в протоколе данным. Однако количество участников, обладающих долями входных и выходных данных, в общем случае может быть меньше количества участников, выполняющих вычисления. Цель – построить протоколы для вычисления линейных и нелинейных функций так, чтобы они могли легко комбинироваться между собой.

Скорость вычислений значительно повышается из-за отказа от искаженных схем при вычислениях нелинейных функций. Традиционный подход состоял в использовании арифметических схем для вычисления линейных функций, применяя тройки Бивера (Beaver’s triplets) и гомоморфное шифрование, а также булевых схем для вычисления нелинейных функций, используя искаженные схемы. Для совмещения двух типов вычислений необходима также конверсия арифметических схем в булевы и обратно, которая требует немалых вычислительных затрат.

Основные криптографические протоколы системы Secure NN следующие:

- трехсторонний протокол умножения матриц, составленных из элементов конечного поля $\mathbb{Z}_{2^k}$, который может быть преобразован в четырехсторонний протокол;
- протокол конфиденциального сравнения разделенного на доли числа x с числом r, который позволяет участникам получить ответ 1, если $x > r$, и 0 в противном случае;
- протокол вычисления старшего бита (MSB) разделенного на доли числа x;
- протокол вычисления функции ReLU(x);
- протокол вычисления производной функции ReLU’(x);
- протокол целочисленного деления разделенных на доли чисел;
- протокол нормализации множества разделенных на доли чисел;
- протокол пулинга по максимальному значению для множества разделенных на доли чисел.

Доказательства криптографической стойкости всех перечисленных протоколов проведены в модели универсальной компонуемости (UC-security).

Система Falcon. Falcon – система КМО на основе трехсторонних протоколов безопасных вычислений, предназначенная для использования на стадиях обучения и применения глубоких нейросетей, поддерживающая, в отличие от ранее известных систем КМО, операцию пакетной нормализации входных данных [22]. Пакетная нормализация

играет существенную роль в обучении нейросетей, позволяя ускорить обучение и улучшить сходимость алгоритмов.

Система Falcon обеспечивает стойкость в модели злоумышленного нарушителя, предполагая, что большинство участников протокола являются честными (т.е. допускается не более одного получестного либо злоумышленного нарушителя). В случае обнаружения воздействия злоумышленного нарушителя выполнение протокола прерывается (англ. security with abort).

Система Falcon основана на идеях SecureNN [3] и ABY^3 [20], используя их в комбинации для повышения производительности. Однако есть и существенные отличия от этих систем. Для обеспечения стойкости к злоумышленному нарушителю вместо (2,2)-пороговой используется (2,3)-пороговая СРС, что приводит к очень существенным изменениям в криптографических примитивах и протоколах.

В системе Falcon реализованы следующие базовые криптографические конструкции, используемые в качестве примитивов:

- вычисление линейных комбинаций разделенных секретов;
- умножение разделенных секретов;
- матричное умножение и вычисление сверток (операция кросс-корреляции) разделенных секретов;
- восстановление секретов из долей;
- протокол выбора долей одного из двух разделенных секретов x или y в зависимости от значения бита выбора c;
- вычисление XOR-суммы разделенного секрета с публично известным битом;
- вычисление долей числового значения вида $(-1)^{\beta} \cdot x$ из долей секретов x и β.

На их основе реализованы следующие криптографические протоколы:

- конфиденциального сравнения разделенного секрета $x \in \mathbb{Z}_p$ с открытым общеизвестным числом r;
- вычисления бита переноса при сложении долей двух и трех разделенных секретов;
- вычисления нелинейных функций активации слоев нейросети ReLU(a) и ее производной DReLU(a) с разделенным секретом a;
- вычисления функции пулинга по максимальному значению $Maxpool(a_1, a_2, \dots, a_n)$ над разделенными секретами $a_1, a_2, \dots, a_n \in \mathbb{Z}_L$, а также производной этой функции;
- вычисления функции целочисленного деления двух разделенных секретов a/b, $a, b \in \mathbb{Z}_L$;
- вычисления функции пакетной нормализации разделенных секретов $a_1, a_2, \dots, a_m \in \mathbb{Z}_L$, где m – размер пакета.

Все протоколы – трехсторонние. Для каждого протокола доказаны теоремы об их криптографической стойкости в модели злоумышленного нарушителя.

Система Attrapadung, Hamada, Ikarashi и др. В [24] описана система КМО, не имеющая собственного наименования, предназначенная для конфиденциального обучения и применения глубоких нейросетей. Она поддерживает достаточно развитые функции и операции, характерные для современных нейросетевых моделей, такие как адаптивная оценка моментов (Adam) и вычисление функций многоклассовой логистической регрессии (softmax), не прибегая к аппроксимациям.

Криптографическая стойкость протоколов обеспечивается в предположении о наличии не более одного получестного или злоумышленного нарушителя.

В системе определены три типа данных:

- двоичные величины – элементы кольца $\mathbb{Z}_2$;
- l-битные целые числа со знаком и без знака;
- l-битные рациональные числа со знаком и без знака.

Для разделения секретных величин используется три вида СРС:

- (2,3)-пороговые СРС над $\mathbb{Z}_p$;
- (2,3)-пороговые СРС над $\mathbb{Z}_2$;
- простое аддитивное разделение секрета над $\mathbb{Z}_p$.

Определяются операции конвертации долей секретов из одной формы представления в другую и восстановления секрета.

Поддерживается следующий набор базовых операций над разделенными секретами:

- протокол деления разделенного секрета на открытый общеизвестный делитель;
- протокол вычисления долей секрета, обратного на множестве рациональных чисел к заданному разделенному секрету;
- протокол деления разделенного секрета на разделенный секретный делитель;
- протокол вычисления $\sqrt{x}$ и $\frac{1}{\sqrt{x}}$ для разделенного секрета x;
- протокол вычисления e^x для разделенного секрета x.

Протоколы могут быть адаптированы для использования на множестве целых чисел со знаком.

Авторы апробировали систему на широко известных глубоких нейросетях AlexNet и VGG16. Эксперименты показали, что быстродействие системы превышает систему Falcon от 10 до 40 раз [22] при показателях точности 70–75% на массиве данных CIFAR-10.

Заключение

В ходе работы выполнено поисковое исследование и проведен обзор существующих систем КМО, которые реализованы преимущественно в виде прототипов и лабораторных образцов. Главное внимание уделено принципам и технологиям реализации систем КМО на основе трехсторонних протоколов безопасных вычислений. Проведен обзор архитектур и математического обеспечения наиболее известных систем КМО, основанных на трехсторонних протоколах безопасных вычислений.

Показано, что основными алгоритмическими инструментами при создании систем КМО на основе трехсторонних протоколов безопасных вычислений служат СРС. В системах КМО используются три вида СРС: арифметическое, булево и Яо-разделения, которые позволяют выполнять безопасные вычисления с разделенными секретами для функций, представленных в форме арифметических, булевых либо искаженных схем соответственно.

Анализ систем КМО на основе трехсторонних протоколов безопасных вычислений позволяет выделить две ведущих линии их развития, сходных с теми, которые были обнаружены при анализе систем КМО на основе двусторонних протоколов безопасных вычислений:

- системы с ядром на основе универсальных программных модулей с набором базовых операций, реализующих произвольную функциональность протокола безопасных вычислений, ограниченную лишь сложностью выполнения протокола (например, модули ABY[3]);
- специализированные КМО с набором криптографических примитивов, оптимизированным для достижения высоких показателей производительности и точности

вычислений, но предназначенных для сравнительно узкого круга методов машинного обучения (например, система CrypTFlow).

Продолжением исследования будет анализ систем КМО на основе четырехсторонних протоколов безопасных вычислений.

СПИСОК ЛИТЕРАТУРЫ:

1. Evans D., Kolesnikov V., Rosulek M. A pragmatic introduction to secure multi-party computation. – 182 p. URL: https://securecomputation.org/docs/pragmaticmpc.pdf (дата обращения: 10.01.2022).
2. Запечников С.В., Щербаков А.Ю. Конфиденциальное машинное обучение на основе двусторонних протоколов безопасных вычислений. Безопасность информационных технологий, [S.I.], т. 28, № 4, 2021, с. 39–51. DOI: http://dx.doi.org/10.26583/bit.2021.4.03.
3. Wagh, S. SecureNN: Efficient and private neural network training. Cryptology ePrint Archive. 2018. – 24 p. URL: https://eprint.iacr.org/2018/442 (дата обращения: 10.01.2022).
4. Chandran N., Gupta D., Rastogi A., Sharma R., Tripathi S. EzPC: Programmable and Efficient Secure Two-Party Computation for Machine Learning. 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden. 2019, p. 496–511. DOI: http://dx.doi.org/10.1109/EuroSP.2019.00043.
5. Kumar E. et al. CrypTFlow: Secure TensorFlow Inference. arXiv preprint. 2020. – 18 p. URL: https://arxiv.org/pdf/1909.07814v2.pdf (дата обращения: 10.01.2022).
6. Rathee D. et al. CrypTFlow2: Practical 2-Party Secure Inference. arXiv preprint. 2020. – 18 p. URL: https://arxiv.org/pdf/2010.06457.pdf (дата обращения: 10.01.2022).
7. Patra A. ABY2.0: Improved mixed-protocol secure two-party computation. A. Patra, T. Schneider, A. Suresh et al. URL: https://ia.cr/2020/1225 (дата обращения: 10.01.2022).
8. Boemer F. MP2ML: a mixed-protocol machine learning framework for private inference. ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security. 2020, p. 1–10. DOI: http://dx.doi.org/10.1145/3407023.3407045. URL: https://dl.acm.org/doi/abs/10.1145/3407023.3407045 (дата обращения: 10.01.2022)
9. Demmler D. ABY – a framework for efficient mixed-protocol secure two-party computation. D. Demmler, T. Schneider, M. Zohner. 22nd Network and Distributed System Security Symposium (NDSS'15), Internet Society, San Diego, CA, USA, February 8–11, 2015. URL: https://encrypto.de/papers/DSZ15.pdf (дата обращения: 10.01.2022).
10. Thien Duc Nguyen, Phillip Rieger, Hossein Yalame, Helen Möllering, Hossein Fereidooni, Samuel Marchal, Markus Miettinen, Azalia Mirhoseini, Ahmad-Reza Sadeghi, Thomas Schneider, and Shaza Zeitouni. FLGUARD: Secure and private federated learning, Jan 6, 2021. URL: https://ia.cr/2021/025 (дата обращения: 10.01.2022).
11. Mishra P. Delphi: A Cryptographic Inference Service for Neural Networks. P. Mishra, R. Lehmkuhl, A. Srinivasan et al. Proc. of USENIX Security 2020 (USENIX Security Symposium). URL: https://www.usenix.org/system/files/sec20spring_mishra_prepub.pdf (дата обращения: 10.01.2022).
12. Raluca Ada Popa homepage: Research. URL: https://people.eecs.berkeley.edu/~raluca/#Research (дата обращения: 10.01.2022).
13. Lehmkuhl R. Muse: Secure Inference Resilient to Malicious Clients. R. Lehmkuhl, P. Mishra, A. Srinivasan et al. Proc. of USENIX Security 2021 (USENIX Security Symposium). URL: https://people.eecs.berkeley.edu/~raluca/MUSEcamera.pdf (дата обращения: 10.01.2022).
14. Rachuri R. Trident: Efficient 4PC framework for privacy preserving machine learning. Cryptology ePrint Archive. 2019. – 26 p. URL: https://eprint.iacr.org/2019/1315 (дата обращения: 10.01.2022).
15. Byali M. FLASH: Fast and robust framework for privacy-preserving machine. Cryptology ePrint Archive. 2019. – 29 p. URL: https://eprint.iacr.org/2019/1365 (дата обращения: 10.01.2022).
16. Patra A. BLAZE: Blazing Fast Privacy-Preserving Machine Learning. Cryptology ePrint Archive. 2020. – 28 p. URL: https://eprint.iacr.org/2020/042.pdf (дата обращения: 10.01.2022).
17. Koti N. SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning. Cryptology ePrint Archive. 2020. – 36 p. URL: https://eprint.iacr.org/2020/592.pdf (дата обращения: 10.01.2022).
18. Koti N. Tetrad: Actively Secure 4PC for Secure Training and Inference. Cryptology ePrint Archive. 2021. – 31 p. URL: https://eprint.iacr.org/2021/755.pdf (дата обращения: 10.01.2022).
19. Mohassel P. SecureML: A system for scalable privacy-preserving machine learning. Cryptology ePrint Archive. 2017. – 38 p. URL: https://eprint.iacr.org/2017/396 (дата обращения: 10.01.2022).
20. Mohassel P. ABY^3: A mixed protocol framework for machine learning. Cryptology ePrint Archive. 2018. – 40 p. URL: https://eprint.iacr.org/2018/403 (дата обращения: 10.01.2022).

21. Mohassel P. Practical privacy-preserving k-means clustering. Cryptology ePrint Archive. 2019. – 30 p. URL: https://eprint.iacr.org/2019/1158 (дата обращения: 10.01.2022).
22. Wagh S. Falcon: Honest-Majority Maliciously Secure Framework for Private Deep Learning. Proc. of Privacy Enhancing Technologies Symposium (PETS), June 2021, p. 1–21. URL: https://arxiv.org/pdf/2004.02229.pdf (дата обращения: 10.01.2022).
23. Sameer W. New directions in efficient privacy-preserving machine learning. Ph. D. Theses. Princeton university. 2020. – 203 p. URL: https://dataspace.princeton.edu/bitstream/88435/dsp01s7526g34f/1/Wagh_princeton_0181D_13320.pdf (дата обращения: 10.01.2022).
24. Attrapadung N. Adam in Private: Secure and Fast Training of Deep Neural Networks with Adaptive Moment Estimation. Cryptology ePrint Archive. 2021. – 24 p. URL: https://eprint.iacr.org/2021/736.pdf (дата обращения: 10.01.2022).
25. Juvekar C. GAZELLE: A Low Latency Framework for Secure Neural Network Inference. Cryptology ePrint Archive. 2021. – 17 p. URL: https://eprint.iacr.org/2018/073.pdf (дата обращения: 10.01.2022).
26. Liu J. Oblivious Neural Network Predictions via MiniONN transformations. Cryptology ePrint Archive. 2017. – 13 p. URL: https://eprint.iacr.org/2017/452.pdf (дата обращения: 10.01.2022).
27. Ryffel T. AriaNN: Low-Interaction Privacy-Preserving Deep Learning via Function Secret Sharing. Preprint. URL: https://arxiv.org/pdf/2006.04593.pdf (дата обращения: 10.01.2022).
28. Mohassel P. Fast and secure three-party computation: The garbled circuit approach. Cryptology ePrint Archive. 2015. – 18 p. URL: https://eprint.iacr.org/2015/931 (дата обращения: 10.01.2022).

REFERENCES:

[1] Evans D., Kolesnikov V., Rosulek M. A pragmatic introduction to secure multi-party computation. – 182 p. URL: https://securecomputation.org/docs/pragmaticmpc.pdf (accessed: 10.01.2022).
[2] Zapechnikov S., Shcherbakov A. Privcy-preserving machine learning based on secure two-party computations. IT Security (Russia), [S.I.], vol. 28, no. 4, 2021, p. 39–51. DOI: http://dx.doi.org/10.26583/bit.2021.4.03 (in Russian).
[3] Wagh, S. SecureNN: Efficient and private neural network training. Cryptology ePrint Archive. 2018. – 24 p. URL: https://eprint.iacr.org/2018/442 (accessed: 10.01.2022).
[4] Chandran N., Gupta D., Rastogi A., Sharma R., Tripathi S. EzPC: Programmable and Efficient Secure Two-Party Computation for Machine Learning. 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden. 2019, p. 496–511. DOI: http://dx.doi.org/10.1109/EuroSP.2019.00043.
[5] Kumar E. et al. CrypTFlow: Secure TensorFlow Inference. arXiv preprint. 2020. – 18 p. URL: https://arxiv.org/pdf/1909.07814v2.pdf (accessed: 10.01.2022).
[6] Rathee D. et al. CrypTFlow2: Practical 2-Party Secure Inference. arXiv preprint. 2020. – 18 p. URL: https://arxiv.org/pdf/2010.06457.pdf (accessed: 10.01.2022).
[7] Patra A. ABY2.0: Improved mixed-protocol secure two-party computation. A. Patra, T. Schneider, A. Suresh et al. URL: https://ia.cr/2020/1225 (accessed: 10.01.2022).
[8] Boemer F. MP2ML: a mixed-protocol machine learning framework for private inference. ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security. 2020, p. 1–10. DOI: http://dx.doi.org/10.1145/3407023.3407045. URL: https://dl.acm.org/doi/abs/10.1145/3407023.3407045 (accessed: 10.01.2022)
[9] Demmler D. ABY – a framework for efficient mixed-protocol secure two-party computation. D. Demmler, T. Schneider, M. Zohner. 22nd Network and Distributed System Security Symposium (NDSS'15), Internet Society, San Diego, CA, USA, February 8–11, 2015. URL: https://encrypto.de/papers/DSZ15.pdf (accessed: 10.01.2022).
[10] Thien Duc Nguyen, Phillip Rieger, Hossein Yalame, Helen Möllering, Hossein Fereidooni, Samuel Marchal, Markus Miettinen, Azalia Mirhoseini, Ahmad-Reza Sadeghi, Thomas Schneider, and Shaza Zeitouni. FLGUARD: Secure and private federated learning, Jan 6, 2021. URL: https://ia.cr/2021/025 (accessed: 10.01.2022).
[11] Mishra P. Delphi: A Cryptographic Inference Service for Neural Networks. P. Mishra, R. Lehmkuhl, A. Srinivasan et al. Proc. of USENIX Security 2020 (USENIX Security Symposium). URL: https://www.usenix.org/system/files/sec20spring_mishra_prepub.pdf (accessed: 10.01.2022).
[12] Raluca Ada Popa homepage: Research. URL: https://people.eecs.berkeley.edu/~raluca/#Research (accessed: 10.01.2022).
[13] Lehmkuhl R. Muse: Secure Inference Resilient to Malicious Clients. R. Lehmkuhl, P. Mishra, A. Srinivasan et al. Proc. of USENIX Security 2021 (USENIX Security Symposium). URL: https://people.eecs.berkeley.edu/~raluca/MUSEcamera.pdf (accessed: 10.01.2022).

[14] Rachuri R. Trident: Efficient 4PC framework for privacy preserving machine learning. Cryptology ePrint Archive. 2019. – 26 p. URL: https://eprint.iacr.org/2019/1315 (accessed: 10.01.2022).
[15] Byali M. FLASH: Fast and robust framework for privacy-preserving machine learning. Cryptology ePrint Archive. 2019. – 29 p. URL: https://eprint.iacr.org/2019/1365 (accessed: 10.01.2022).
[16] Patra A. BLAZE: Blazing Fast Privacy-Preserving Machine Learning. Cryptology ePrint Archive. 2020. – 28 p. URL: https://eprint.iacr.org/2020/042.pdf (accessed: 10.01.2022).
[17] Koti N. SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning. Cryptology ePrint Archive. 2020. – 36 p. URL: https://eprint.iacr.org/2020/592.pdf (accessed: 10.01.2022).
[18] Koti N. Tetrad: Actively Secure 4PC for Secure Training and Inference. Cryptology ePrint Archive. 2021. – 31 p. URL: https://eprint.iacr.org/2021/755.pdf (accessed: 10.01.2022).
[19] Mohassel P. SecureML: A system for scalable privacy-preserving machine learning. Cryptology ePrint Archive. 2017. – 38 p. URL: https://eprint.iacr.org/2017/396 (accessed: 10.01.2022).
[20] Mohasse P. ABY^3: A mixed protocol framework for machine learning. Cryptology ePrint Archive. 2018. – 40 p. URL: https://eprint.iacr.org/2018/403 (accessed: 10.01.2022).
[21] Mohassel P. Practical privacy-preserving k-means clustering. Cryptology ePrint Archive. 2019. – 30 p. URL: https://eprint.iacr.org/2019/1158 (accessed: 10.01.2022).
[22] Wagh S. Falcon: Honest-Majority Maliciously Secure Framework for Private Deep Learning. Proc. of Privacy Enhancing Technologies Symposium (PETS), June 2021, p. 1–21. URL: https://arxiv.org/pdf/2004.02229.pdf (accessed: 10.01.2022).
[23] Sameer W. New directions in efficient privacy-preserving machine learning. Ph. D. Theses. Princeton university. 2020. – 203 p. URL: https://dataspace.princeton.edu/bitstream/88435/dsp01s7526g34f/1/Wagh_princeton_0181D_13320.pdf (accessed: 10.01.2022).
[24] Attrapadung N. Adam in Private: Secure and Fast Training of Deep Neural Networks with Adaptive Moment Estimation. Cryptology ePrint Archive. 2021. – 24 p. URL: https://eprint.iacr.org/2021/736.pdf (accessed: 10.01.2022).
[25] Juvekar C. GAZELLE: A Low Latency Framework for Secure Neural Network Inference. Cryptology ePrint Archive. 2021. – 17 p. URL: https://eprint.iacr.org/2018/073.pdf (accessed: 10.01.2022).
[26] Liu J. Oblivious Neural Network Predictions via MiniONN transformations. Cryptology ePrint Archive. 2017. – 13 p. URL: https://eprint.iacr.org/2017/452.pdf (accessed: 10.01.2022).
[27] Ryffel T. AriaNN: Low-Interaction Privacy-Preserving Deep Learning via Function Secret Sharing. Preprint. URL: https://arxiv.org/pdf/2006.04593.pdf (accessed: 10.01.2022).
[28] Mohassel P. Fast and secure three-party computation: The garbled circuit approach. Cryptology ePrint Archive. 2015. – 18 p. URL: https://eprint.iacr.org/2015/931 (accessed: 10.01.2022).

Поступила в редакцию – 11 января 2022 г. Окончательный вариант – 27 января 2022 г.
Received – January 11, 2022. The final version – January 27, 2022.

Сергей Н. Горячев[1], Николай С. Кобяков[2]
Пермский военный институт войск национальной гвардии Российской Федерации,
ул. Гремячий Лог, 1, Пермь, 614112, Россия
[1]*e-mail: sergory@mail.ru, https://orcid.org/0000-0002-6994-8559*
[2]*e-mail: kkobyakov1234@gmail.com, https://orcid.org/0000-0002-4950-7879*

ОЦЕНКА СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

DOI: http://dx.doi.org/10.26583/bit.2022.1.05

Аннотация. В данной статье рассмотрены основные виды вредоносных программ и их деструктивное воздействие на информационные системы. Целью работы является разработка математической модели для оценки состояния защищенности информационных систем на основе структурно-функционального анализа. Для достижения цели работы проанализированы существующие математические модели адаптивного управления защитой информации, построен граф вероятности состояний и переходов системы. Определены понятия состояний системы и их зависимость от необходимых и достаточных условий возникновения и протекания процесса заражения вредоносной программой. Исследована зависимость состояния информационной системы от различных детерминированных и стохастических событий. Разработана модель системы защиты информационной системы от вредоносных программ, определены допустимые значения опасных факторов вредоносных программ. Данная модель может использоваться специалистами в области защиты информации для оценки защищенности как введенных в эксплуатацию информационных систем, так и при разработке систем.

Ключевые слова: информационная система, вредоносная программа, структурно-функциональный анализ, защита систем.

Для цитирования: ГОРЯЧЕВ, Сергей Н.; КОБЯКОВ, Николай С. ОЦЕНКА СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 44–56, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1401. DOI: http://dx.doi.org/10.26583/bit.2022.1.05.

Sergey N. Goryachev[1], Nikolai S. Kobyakov[2]
Perm military Institute of National Guard Troops,
Gremyachiy Log Str., 1, Perm, 614112, Russia
[1]*e-mail: sergory@mail.ru, https://orcid.org/0000-0002-6994-8559*
[2]*e-mail: kkobyakov1234@gmail.com, https://orcid.org/0000-0002-4950-7879*

Assessment of the state of protection of information systems against malware

DOI: http://dx.doi.org/10.26583/bit.2022.1.05

Abstract. This paper discusses the main types of malware and their destructive effects on information systems. The current work develops a mathematical model for assessing the state of security of information systems based on structural and functional analysis. To achieve the goal of this work, we analyzed existing mathematical models of adaptive information security management, and built a probability graph of system states and transitions. We define the concept of system states and their dependence on the necessary and sufficient conditions for the emergence and duration of the process of destruction by malware. The dependence of information system states on various deterministic and stochastic events has been studied. A model of a system for protecting an information system from malicious programs has been developed, and the permissible values of dangerous factors of malicious programs have been determined. The result of this work is a mathematical model for assessing the state of protection of an information system from malware. This model can be used by specialists in the field of information security to assess the security of both the operating information systems and those under development.

Keywords: information system, malware, structural and functional analysis, protection of an information system.
For citation: GORYACHEV, Sergey N.; KOBYAKOV, Nikolai S. Assessment of the state of protection of information systems against malware. IT Security (Russia), [S.l.], v. 29, n. 1, p. 44–56, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1401. DOI: http://dx.doi.org/10.26583/bit.2022.1.05.

Введение

Информационная система (ИС) – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.[1] В настоящее время в связи с увеличением количества хакерских атак на российские государственные органы есть необходимость использовать информационные системы специального назначения (ИССН). Поскольку российские государственные органы являются органами государственной исполнительной власти, то циркулирующая в ИС информация представляет интерес для многих сторон, начиная с криминальных группировок, и заканчивая отдельными физическими лицами, имеющими корыстные или иные цели [1]. В этих условиях все больше востребованными в повседневной деятельности российских государственных органов становятся вопросы управления обеспечением защиты ИС, исходя из требований конфиденциальности, целостности и доступности к информации. Вместе с тем в документах государственных регуляторов сегодня отсутствуют требования к управлению безопасностью ИССН в части касающейся защиты от угрозы применения вредоносных программ (ВП). Действующие нормативные документы, например, ФСТЭК России, регламентируют применение положений ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Руководство по менеджменту безопасности» и ряда других ГОСТов, где декларируются обязанности должностных лиц и требования к информационным системам в целом. При этом в этих положениях не учитывается динамичность информационных процессов реализации угроз и защита от них. В частности, в них не учитывается динамика опасных последствий (нарушения работы прикладных программ, разрушение, искажение файлов и т.д.) от деструктивных функций ВП. В [2, 3] рассмотрены вопросы создания моделей управления системой защиты информации, а в [4, 5] разработаны модели оценки эффективности функционирования подсистем системы защиты информации, но, не рассмотрена возможность использования структурно-функционального анализа для решения задачи оценки состояния защищенности.

1. Основная часть исследования

Учет динамики процессов внедрения ВП со своевременной реакцией управления защитой информации в ИССН может не только существенно повлиять на эффективность защиты информации, но и изменить требования к защите. Однако для такого учёта необходимо иметь модели адаптивного управления защитой информации, направленной на своевременное обнаружение, нейтрализацию и прогнозирование последствий от деструктивных функций ВП в ИССН в условиях динамики реализации угроз ее безопасности.

Решением задачи является разработка модели адаптивного управления защитой информации в ИССН. Далее рассмотрим задачу определения показателя безопасности ИС при воздействии ВП на основе применения системного подхода.

[1]Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»// СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 01.12.2021).

Сущность системного подхода состоит в том, что объект проектирования или управления рассматривается как система, т.е. как единство взаимосвязанных элементов, которые образуют единое целое и действуют в интересах реализации единой цели [6].

Основные положения системного подхода:

1) любой объект – это открытая система, взаимодействующая с внешней средой;
2) эффективность функционирования системы определяется ее системными качествами и условиями окружающей среды;
3) элементы системы рассматриваются в их взаимосвязи.

Защита информации в ИССН от деструктивного воздействия ВП представляет собой постоянный процесс, выполняемый на всех этапах жизненного цикла информации (хранение, обработка и передача) при комплексном использовании всех имеющихся средств и методов защиты. При этом все средства, методы и мероприятия, применяемые для защиты информации, объединяются в единый целостный механизм.

Объектом в данном случае является ИС, в которой поставленные цели могут быть полностью достигнуты в результате решения следующих задач: выявление ВП, определение и прогнозирование последствий от деструктивных функций ВП, воздействующих или могущие воздействовать на защищаемую информацию. Решение данных задач составляет основу для эффективного управления защитой информации в конкретных условиях.

2. Построение графа модели состояний

ВП могут иметь следующие особенности:

– скрытие признаков своего присутствия;
– маскирование себя под прикладное программное обеспечение;
– перенос своих фрагментов в области оперативного и постоянного запоминающих устройств;
– нечеткая идентификация кода ВП;

На основе анализа указанных особенностей развития и реализации угроз ВП в ИС, построена модель взаимосвязей элементов исследуемой ИС.

Для формализации элементов системы введем следующие множества (рис. 1):

$C = \{ c_1, c_2, ..., c_n \}$ – множество информационных систем;

$V = \{v_1, v_2, ..., v_n\}$ – семейство вредоносных программ;

$E = \{e_1, e_2, ..., e_n\}$ – множество элементов сетевой инфраструктуры;

$U = \{u_1, u_2, ..., u_n\}$ – множество элементов управления.

Данного набора множеств достаточно, для описания основных элементов, от которых зависит функционирование ИССН.

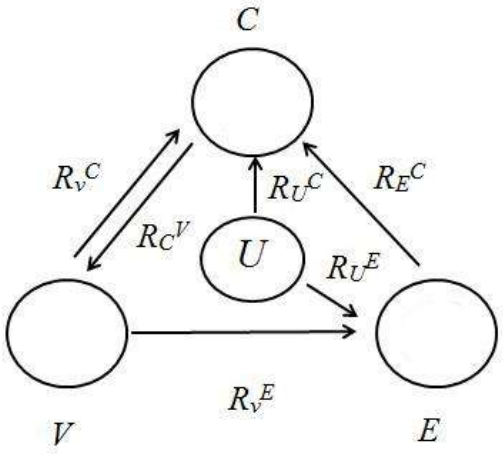


Рис. 1. Взаимосвязь элементов исследуемой системы
Fig. 1. The relationship of the elements of the system studied

Элементы системы S будут взаимосвязаны бинарными отношениями R (1), под которыми можно понимать функциональные отношения, предпочтения, следования и другие, отражающие существо взаимосвязи элементов системы. Например, семейство вредоносных программ V воздействует на ИС C отношением $VR_V^C C$, реагирование C на V определяется $CR_C^V V$:

$$VR_V^C C,\ VR_V^E E,\ CR_C^V V,\ ER_E^C C,\ UR_U^C C,\ UR_U^E E. \quad (1)$$

Разложим бинарные отношения R на два подмножества: незараженный (1) и зараженный (2) файл [7]. Файл, как структурированный объект, находится в некоторых условиях, определяемых операционной системой сервера или пользователем ИС. В этом случае система (1) преобразуется следующим образом:

$$VR_V^{C1}[S_C^V, C^1],\ S_C^V R_V^{C2} C^2\ ;\ VR_V^{E1}[S_E^V, E^1],\ S_E^V R_V^{E2} E^2;\ ER_E^{C1}[S_V^E, C^1],\ S_V^E R_E^{C2} C^2;$$
$$CR_C^{V1}[S_{V1}^C, V^1],\ S_{V2}^C R_C^{V2} V^2;\ UR_U^{C1}[S_{C1}^U, C^1],\ S_{C2}^U R_U^{C2} C^2;\ UR_U^{E1}[S_{E1}^U, E^1],\ S_{E1}^U R_U^{E2} E^2. \quad (2)$$

Состояния системы S каждого элемента зависят от их свойств, которые изменяются во время жизненного цикла системы. Состояние безопасности ИС S_C зависит от собственных свойств Q_C –наличие уязвимостей, настройки разграничений прав доступа пользователей (администратора), архитектуры и программной реализации ИС, наличие антивирусной программы, параметров сетевой инфраструктуры и деструктивных возможностей ВП

$$S_C = F_1[\{Q_C\}, S_C^E, S_C^V]. \quad (3)$$

Состояние сетевой инфраструктуры S_E зависит от собственных свойств инфраструктуры Q_E – топологии сети, состава сетевого оборудования, функциональных возможностей ВП

$$S_E = F_2\{Q_E\}, S_E^V. \quad (4)$$

Состояние ВП S_V зависит от собственных свойств ВП Q_V – скорости и способа распространения, состава деструктивного функционала

$$S_V = F_3\{Q_V\}. \quad (5)$$

Состояние ИС определяется свойствами элементов S_C, S_E, S_V. Характер изменения этих свойств в процессе жизненного цикла ИС, как правило, изменяется из-за обработки, хранения и передачи информации между пользователями. Таким образом, модель оценки состояния элементов системы *CE* опишется некоторым функционалом $\Im$

$$S_{CE} = \Im\,[S_C, S_E, S_V]. \tag{6}$$

3. Исследование модели оценки состояния информационной системы

Исследуем более подробно безопасность ИС. Под безопасностью ИС понимается непрерывная функция в диапазоне от 0 до 1, дифференцируемая на всей области определения. Изменение состояния безопасности файловой структуры (*P*) ИС опишется следующей зависимостью, (взаимосвязь данных элементов представлена на рис. 1)

$$S_C = \Delta P_C\left(Q_C\right) + \Delta P_C\left(E\right) + \Delta P_C\left(V\right), \tag{7}$$

где $\Delta P_C(Q_C)$ – изменение показателя безопасности ИС от выявленных собственных уязвимостей, $\Delta P_C(E)$ – изменение показателя безопасности ИС от сетевой инфраструктуры, $\Delta P_C(V)$ – изменение показателя безопасности ИС от воздействий ВП.

Под уязвимостями безопасности ИС можно понимать свойства элементов файловой структуры ИС: тип *Tp*, атрибуты *At*, настройки матрицы доступа *Mt* и размеры *Ob* файлов

$$\Delta P_C\left(Q_C\right) = \frac{\partial P_C}{\partial Q_{Tp}}\Delta Q_{Tp} + \frac{\partial P_C}{\partial Q_{At}}\Delta Q_{At} + \frac{\partial P_C}{\partial Q_{Mt}}\Delta Q_{Mt} + \frac{\partial P_C}{\partial Q_{Ob}}\Delta Q_{Ob}. \tag{8}$$

От параметров сетевой инфраструктуры зависит активность ВП, например, демилитаризованной зоны *Dmz*, межсетевого экрана *Mn*, криптографических защищенных сетевых протоколов *Kvp*

$$S_E = \Delta P_C\left(E\right)$$

$$\Delta P_C\left(E\right) = \frac{\partial P_C}{\partial E_{Dmz}}\Delta E_{Dmz} + \frac{\partial P_C}{\partial E_{Mn}}\Delta E_{Mn} + \frac{\partial P_C}{\partial E_{Kvp}}\Delta E_{Kvp}. \tag{9}$$

Изменение показателя опасности $\Delta Q_C(V)$ зависит от группы вредоносных программ и опишется уравнением

$$S_V = \Delta Q_C(\mathrm{V})$$

$$\Delta Q_C\left(V\right) = \frac{\partial Q_C}{\partial v_1}\Delta v_1 + \frac{\partial Q_C}{\partial v_2}\Delta v_2 + \frac{\partial Q_C}{\partial v_3}\Delta v_3 + \frac{\partial Q_C}{\partial v_4}\Delta v_4 \tag{10}$$

где:

v_1={файловые вирусы, макровирусы, загрузочные вирусы} – множество ВП 1-го типа;

v_2={программные закладки} – множество ВП 2-го типа;

v_3={ВП, распространяющиеся по сети } – множество ВП 3-го типа;

v_4={ другие вредоносные программы } – множество ВП 4-го типа.

Современные ВП основаны на использовании уязвимостей системного и прикладного программного обеспечения, технологий обработки информации, протоколов передачи данных. Они обладают широким спектром деструктивных возможностей [8].

Пример работы вредоносных программ представлен на рис. 2 [9].

Рис. 2. Результат действия вредоносных программ
Fig. 2. The result of the action of malware

Обобщённый функционал деструктивных функций (dsf) вредоносных программ может быть представлен в следующем виде

$$\Delta v\ (\mathrm{dsf}) = \frac{\partial v}{\partial(\mathrm{dsf}_1)}\Delta\mathrm{dsf}_1 + \frac{\partial v}{\partial(\mathrm{dsf}_2)}\Delta\mathrm{dsf}_2 + \frac{\partial v}{\partial(\mathrm{dsf}_3)}\Delta\mathrm{dsf}_3 + \frac{\partial v}{\partial(\mathrm{dsf}_4)}\Delta\mathrm{dsf}_4 +$$
$$+ \frac{\partial v}{\partial(\mathrm{nsp}_5)}\Delta\mathrm{dsf}_5 + \frac{\partial v}{\partial(\mathrm{dsf}_6)}\Delta\mathrm{dsf}_6 + \frac{\partial v}{\partial(\mathrm{dsf}_7)}\Delta\mathrm{dsf}_7 + \frac{\partial v}{\partial(\mathrm{dsf}_8)}\Delta\mathrm{dsf}_8 + \frac{\partial v}{\partial(\mathrm{dsf}_9)}\Delta\mathrm{dsf}_9 + \quad (11)$$
$$+ \frac{\partial v}{\partial(\mathrm{dsf}_{10})}\Delta\mathrm{dsf}_{10} + \frac{\partial v}{\partial(\mathrm{dsf}_{11})}\Delta\mathrm{dsf}_{11} + \frac{\partial v}{\partial(\mathrm{dsf}_{12})}\Delta\mathrm{dsf}_{12},$$

где:
dsf_1 – уничтожение данных в секторах постоянного запоминающего устройства;
dsf_2 – исключение возможности загрузки операционной системы;
dsf_3 – искажение кода загрузчика операционной системы;
dsf_4 – форматирование логических дисков постоянного запоминающего устройства;
dsf_5– закрытие (открытие) доступа к портам (COM, USB, RJ-45 и др.);
dsf_6 – закрытие (открытие) логических портов компьютера;
dsf_7 – замена символов при печати текстов;
dsf_8 – создание звуковых (визуальных) эффектов на экране монитора;
dsf_9 – искажение файлов данных;
dsf_{10} – перезагрузка системы;
dsf_{11} – шифрование файлов данных пользователя (.doc, .docx, .docm, .dot, .xls, .pptx, .ppt, .jpg, .jpeg и др.);
dsf_{12} – шифрование системных файлов (.drv, .sys, .com, .exe, csr, .pem, .key и др.).

4. Разработка графа состояний и переходов

Необходимым условием для реализации угрозы заражения вредоносной программой является наличие вредоносной программы S_V на автоматизированном рабочем месте, а достаточным – отсутствие антивирусной программы и файрвола *b*, отсутствие контроля над подключением съемных носителей *r* и времени воздействия *o*.

Наличие вредоносной программы необходимо для реализации угрозы, так как если ее не будет, то и не будет существовать угрозы заражения вредоносной программой. В свою очередь, если на автоматизированном рабочем месте будут реализованы меры

защиты (установлены файрвол, антивирусная программа, осуществлен контроль над подключением съемных носителей), то угроза заражения вредоносной программой будет минимизирована. Кроме того, вредоносной программе для деструктивного воздействия необходимо время.

В табл. 1 представлены необходимые и достаточные условия возникновения и протекания процесса заражения вредоносными программами в информационной системе.

Таблица 1. Необходимые и достаточные условия возникновения и протекания процесса заражения вредоносной программой

Вероятность состояния	Вид состояния	Параметры
p_1	Безопасное состояние (отсутствие необходимого и достаточных условий)	$\mathrm{C}^1 = \begin{pmatrix} S_V < S_V^d \\ b < b^d \\ o < o^d \\ r < r^d \end{pmatrix}$
p_2	Опасное состояние воздействия на информационную систему (есть необходимое (S_V), но отсутствуют достаточные условия)	$\mathrm{C}^2 = \begin{pmatrix} S_V > S_V^d \\ b < b^d \\ o < o^d \\ r < r^d \end{pmatrix}$
p_3	Состояние заражения вредоносной программой (присутствие необходимого (S_V) и достаточных условий (b,r))	$\mathrm{C}^3 = \begin{pmatrix} S_V < S_V^d \\ b > b^d \\ o < o^d \\ r > r^d \end{pmatrix}$
p_4	Состояние нарушения работоспособности информационной системы (присутствие необходимого (S_V) и достаточных условий (b, o, r))	$\mathrm{C}^4 = \begin{pmatrix} S_V < S_V^d \\ b > b^d \\ o > o^d \\ r < r^d \end{pmatrix}$

где S_V^d, b_d, o_d, r_d предельно допустимые параметры распространения вредоносной программы.

Для модели переходных состояний предлагается использовать полумарковские процессы, так как они характеризуются произвольными функциями распределения p_i. Под воздействием активности вредоносной программы с вероятностью перехода λ_{ij} происходит переход системы из состояния C_i в состояние C_j. Определение вероятности $p_i(t)$ состояния системы определяется решением системы уравнений Колмогорова.

$$\frac{\partial p_i}{\partial t} = \sum_{j=1}^{n} \lambda_{ij} p_j(t) - p_i(t) \sum_{j=1}^{n} \lambda_{ij}, (i = 1,2,3,\ldots,n) \qquad (12)$$

с начальными условиями $p_i(0) \geq 0$, $\sum_{i=1}^{n} p_i(0) = 1$.

Исходя из вышеприведенного, система с точки зрения безопасности информационной системы к заражению вредоносными программами может находиться в одном из четырех состояний:

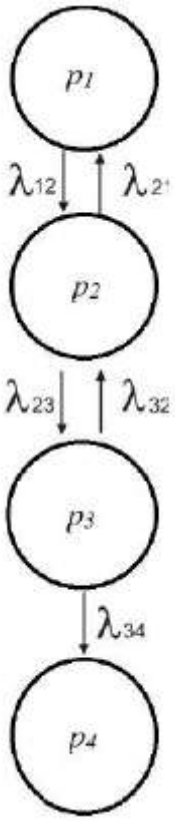
C^1 – безопасное состояние, когда в системе отсутствуют необходимые условия заражения вредоносной программой;

C^2 – состояние опасной ситуации, когда в системе существует вредоносная программа, но отсутствуют достаточные условия заражения вредоносной программой;

C^3 – состояние зараженного компьютера, когда программа начинает свою деятельность;

C^4 – состояние нарушения работоспособности информационной системы.

Взаимосвязи между вероятностными состояниями системы представлены на рис. 1, из которого видно, что система может переходить из безопасного состояния p_1 в опасное p_2 и далее в зараженное p_3 состояния или обратные переходы при установке антивирусного программного обеспечения и принятия своевременных мер по уничтожению вредоносных программ. Переход из зараженного состояния в состояние нарушения работоспособности p_4 – конечный, так как работа информационной системы в этот момент нарушена. Система дифференциальных уравнений для графа вероятностей состояний p_i и переходов λ_{ij} системы показана на рис. 3.



$$\frac{\partial p_1(t)}{\partial t} = \lambda_{21} p_2(t) - \lambda_{12} p_1(t)$$

$$\frac{\partial p_2(t)}{\partial t} = \lambda_{12} p_1(t) + \lambda_{32} p_3(t) - \lambda_{21} p_2(t) - \lambda_{23} p_2(t)$$

$$\frac{\partial p_3(t)}{\partial t} = \lambda_{23} p_2(t) - \lambda_{32} p_3(t) - \lambda_{34} p_3(t)$$

$$\frac{\partial p_4(t)}{\partial t} = \lambda_{34} p_3(t)$$

Рис. 3. Граф вероятности состояний p_i и переходов λ_{ij} системы
Fig. 3. Graph of the probability of constructing p_i and transitions λ_{ij} of the system

5. Построение модели системы защиты информации информационных систем

Формализация пространства параметров опасности *i* вредоносной программы позволяет оценить степень безопасности информационной системы уравнением

$$\theta_i = \begin{cases} \frac{1}{4}\left(\frac{S_{V\,i}^{\,d} - S_{V\,i}}{S_{V\,i}^{\,d}} + \frac{b_i - b_i^d}{b_i^d} + \frac{r_i^d - r_i}{r_i^d} + \frac{o_i^d - o_i}{o_i^d} \right), \text{при } \left(S_{V\,i} < S_{V\,i}^{\,d}\right) \wedge \left(b_i > b_i^d\right) \wedge \left(r_i < r_i^d\right) \wedge \left(o_i < o_i^d\right); \\ 0, \quad \text{при } \left(S_{V\,i} \geq S_{V\,i}^{\,d}\right) \vee \left(b_i < b_i^d\right) \vee \left(o_i > o_i^d\right) \vee \left(r_i > r_i^d\right). \end{cases} \quad (13)$$

Таким образом, общий показатель для множества источников вредоносных программ рассчитывается как среднее арифметическое или равен нулю, если хотя бы один из источников вредоносных программ опасен (14).

$$\Theta = \begin{cases} \frac{1}{N}\sum_{i=1}^{N} \theta_i, \forall\, i = \overline{1, N} : \theta_i > 0; \\ 0 \qquad , \exists\, i = \overline{1, N} : \theta_i = 0. \end{cases} \quad (14)$$

В процессе функционирования информационной системы параметры источников вредоносных программ (*c, b, r, o*) системы могут изменяться, как детерминировано, так и стохастически, и представлены [10]

$$S_V = S_V\left(\vartheta_{SV}(t), t\right),\ b = b\left(\vartheta_b(t), t\right),\ \ r = r\left(\vartheta_r\ (t), t\right),\ o = \left(\vartheta_o(t), t\right), \quad (15)$$

где $\vartheta(t)$ – случайное событие.

Дифференцируя сложные функции (16), получим

$$\begin{gathered} \frac{\partial cv(\vartheta_{SV}(t), t)}{\partial t} = \frac{\partial S_V(\vartheta_{SV}(t))}{\partial \vartheta_{SV}(t)} \cdot \frac{\partial(\vartheta_{SV}(t)}{\partial t} + \frac{\partial S_V(t)}{\partial t} \\ \frac{\partial b(\vartheta_b(t), t)}{\partial t} = \frac{\partial x(\vartheta_b(t))}{\partial \vartheta_b(t)} \cdot \frac{\partial \vartheta_b(t)}{\partial t} + \frac{\partial b(t)}{\partial t} \\ \frac{\partial r(\vartheta_r(t), t)}{\partial t} = \frac{\partial r(\vartheta_r(t))}{\partial \vartheta_r(t)} \cdot \frac{\partial \vartheta_r(t)}{\partial t} + \frac{\partial r(t)}{\partial t} \\ \frac{\partial o(\vartheta_o(t), t)}{\partial t} = \frac{\partial o(\vartheta_o(t))}{\partial \vartheta_o(t)} \cdot \frac{\partial \vartheta_o(t)}{\partial t} + \frac{\partial o(t)}{\partial t} \end{gathered} \quad (16)$$

где $\frac{\partial S_V\left(\vartheta_{SV}(t)\right)}{\partial \vartheta_{SV}(t)}, \frac{\partial b(\vartheta_b(t))}{\partial \vartheta_b(t)}, \frac{\partial r(\vartheta_r(t))}{\partial \vartheta_r(t)}, \frac{\partial t(\vartheta_o(t))}{\partial \vartheta_o(t)}$ - плотности распределения вероятностей случайной величины заражения вредоносной программой информационной системы;

$\frac{\partial S_V(t)}{\partial t}, \frac{\partial b(t)}{\partial t}, \frac{\partial r(t)}{\partial t}, \frac{\partial o(t)}{\partial t}$ - функции детерминированного изменения параметров вредоносной программы;

$\frac{\mathrm{d}\vartheta_{SV}(t)}{\mathrm{d}t}, \frac{\mathrm{d}\vartheta_b(t)}{\mathrm{d}t}, \frac{\mathrm{d}\vartheta_r(t)}{\mathrm{d}t}, \frac{\mathrm{d}\vartheta_o(t)}{\mathrm{d}t}$ - плотности распределения времени наступления заражения информационной системы.

В случае нормального закона распределения случайной величины при экспоненциальном законе времени нарушения работоспособности информационной системы λ получим следующие выражения:

$$S_V(t) = \int_0^t \frac{\partial S_V(\vartheta_{SV}(t), t)}{\partial t}\partial t$$

$$= \int_0^t \left(\frac{1}{\sigma_{cv}\sqrt{2\pi}} exp\left(-\left[\frac{\vartheta_{SV} - M(\vartheta_{SV})}{2\sigma_{cv}}\right]^2\right) exp(\lambda_{SV} t)\, \partial t + \int_0^t \frac{\partial S_V(t)}{\partial t}\partial t\right.$$

$$= S_V(t) + \frac{1}{\sigma_{cv}\sqrt{2\pi}} exp\left(-\left[\frac{\vartheta_{SV} - M(\vartheta_{SV})}{2\sigma_{cv}}\right]^2\right) \exp(-\lambda_{SV} t)$$

$$b(t) = b(t) + \left(-\left[\frac{\vartheta_b - M(\vartheta_b)}{2\sigma_b}\right]^2\right) \exp(-\lambda_b t) \quad (17)$$

$$r(t) = r(t) + \frac{1}{\sigma_r\sqrt{2\pi}}\left(-\left[\frac{\vartheta_b - M(\vartheta_b)}{2\sigma_b}\right]^2\right) \exp(-\lambda_r t)$$

$$o(t) = o(t) + \frac{1}{\sigma_o\sqrt{2\pi}} exp\left(-\left[\frac{\vartheta_b - M(\vartheta_b)}{2\sigma_b}\right]^2\right) \exp(-\lambda_o t)$$

При известных законах распределения случайной величины с помощью системы уравнений (17) можно определить вероятность заражения информационной системы вредоносной программой с целью принятия мер по созданию системы защиты [11, 12].

В настоящее время ведутся активные работы по защите информационных систем от вредоносных программ [13]. На рис. 4 приведена модель системы защиты информационной системы.

Защита L должна обеспечивать воздействие от опасных факторов вредоносных программ не выше допустимых значений:

$$L_{SV} * S_V(t), L_b * b(t), L_r * r(t), L_o * o(t)\,. \quad (18)$$

Безопасность системы (рис. 4) по параметрам источника опасности вредоносных программ будет обеспечиваться в случае выполнения неравенств:

$$S_V^d - L_{SV} \cdot S_V(t) \geq 0, L_b \cdot b(t) - b^d \geq 0, r^d - L_r \cdot r(t) \geq 0, o^d - L_o \cdot o(t) \geq 0. \quad (19)$$

Оценка безопасности системы по i-му источнику опасности вредоносных программ с учетом коэффициентов защиты будет определяться по выражению (18) с учетом выполнения неравенств (19):

$$\theta_i = \frac{1}{4}\left[\left(\frac{S_{Vi}^d - L_{SVi} \cdot c_i(t)}{S_{Vi}^d}\right) + \left(\frac{L_{bi} b_i(t) - b_i^d}{b_i^d}\right) + \left(\frac{r_i^d - L_{ri} \cdot r(t)}{r_i^d}\right) + \left(\frac{o_i^d - L_{oi} \cdot o(t)}{o_i^d}\right)\right]$$

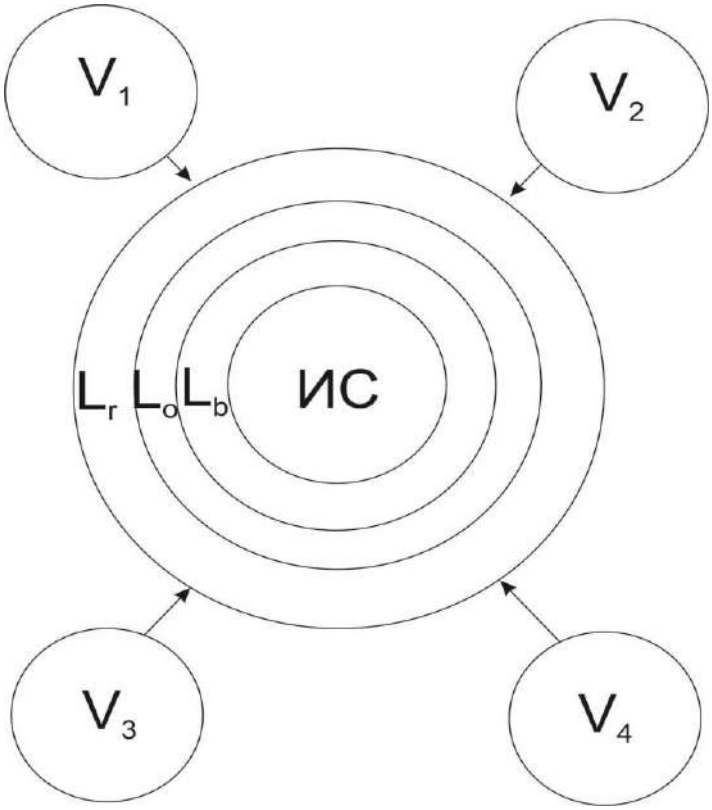


Рис. 4. Модель системы защиты информационной системы
Fig. 4. Model of the system to protect the information system

Защита L должна обеспечить воздействие опасных факторов вредоносных программ не выше допустимых значений, ее можно определить как средства и мероприятия борьбы с вредоносными программами, снижающие значения параметров до допустимых значений (20)

$$L_b \geq \frac{\theta_i^d}{\theta_i},\ L_r \leq \frac{\theta_i^d}{\theta_i},\ L_{SV} \leq \frac{\theta_i^d}{\theta_i},\ L_r \leq \frac{\theta_i^d}{\theta_i}, \quad (20)$$

где θ_i^d – допустимое значение величины источника вредоносных программ.

Разработка и внедрение данной модели позволит своевременно и надежно отслеживать состояние информационной системы.

Заключение

Вопрос защиты информационных систем становится все более актуальным с развитием информационных технологий. Для качественной оценки состояния защищенности информационных систем необходимо в руководящих документах определить требования к управлению безопасностью в ИССН. В данной работе определены взаимосвязи элементов, участвующих в процессе обработки и защиты информации, представлен граф состояний и переходов с учетом достаточных и необходимых условий для заражения вредоносной программой. Разработана математическая модель для оценки состояния защищенности информационной системы от вредоносных программ с учетом коэффициентов защиты. По результатам работы

может быть разработана методика оценки состояния защищенности информационных систем от вредоносных программ.

СПИСОК ЛИТЕРАТУРЫ:

1. Смирнов В.М., Киселёв С.А. Вредоносные программы как опасность ОВД. Shape * MERGEFORMAT. Евразийский Союз Ученых. 2020, № 3-1 (72), с. 43–44. URL: https://cyberleninka.ru/article/n/vredonosnye-programmy-kak-opasnost-ovd-shape-mergeformat (дата обращения: 01.12.2021).
2. Голдобина А.С., Исаева Ю.А., Селифанов В.В., Климова А.М., Зенкин П.С. Построение адаптивной трехуровневой модели процессов управления системой защиты информации объектов критической информационной инфраструктуры. Доклады ТУСУР. 2018, № 4, с. 51–58. URL: https://cyberleninka.ru/article/n/postroenie-adaptivnoy-trehurovnevoy-modeli-protsessov-upravleniya-sistemoy-zaschity-informatsii-obektov-kriticheskoy (дата обращения: 01.12.2021).
3. Бабенко А.А., Козунова С.С. Модель управления защитой информации в государственных информационных системах. NBI-technologies. 2018, № 4, с. 16–22. URL: https://cyberleninka.ru/article/n/model-upravleniya-zaschitoy-informatsii-v-gosudarstvennyh-informatsionnyh-sistemah (дата обращения: 01.12.2021).
4. Бацких А.В., Дровникова И.Г. Модель и алгоритм оценки эффективности функционирования подсистемы управления доступом системы защиты информации от несанкционированного доступа в автоматизированных системах органов внутренних дел. Вестник ВИ МВД России. 2021, № 2, с. 34–45. URL: https://cyberleninka.ru/article/n/model-i-algoritm-otsenki-effektivnosti-funktsionirovaniya-podsistemy-upravleniya-dostupom-sistemy-zaschity-informatsii-ot (дата обращения: 01.12.2021).
5. Бацких А.В. Имитационная модель процесса функционирования модифицированной подсистемы управления доступом системы защиты информации от несанкционированного доступа в программном окружении CPN TOOLS. Вестник ВИ МВД России. 2020, № 3, с. 96–106. URL: https://cyberleninka.ru/article/n/imitatsionnaya-model-protsessa-funktsionirovaniya-modifitsirovannoy-podsistemy-upravleniya-dostupom-sistemy-zaschity-informatsii-ot (дата обращения: 01.12.2021).
6. Антонов А.В. Системный анализ: учеб. для вузов. А.В. Антонов. М.: Наука и технологии, 2008. – 177 с.
7. Курош А.Г. Курс высшей алгебры. А.Г. Курош. СПб.: Лань, 2006. – 432 с.
8. Смирнов В.М., Цыганкова Я.В., Нестеров И.А. Состояние и тренды сетевой безопасности. Евразийский Союз Ученых. 2019, № 9-2 (66), с. 42–43. URL: https://cyberleninka.ru/article/n/sostoyanie-i-trendy-setevoy-bezopasnosti (дата обращения: 30.11.2021).
9. Вирус-шифровальщик. xakep.ru. URL: https://xakep.ru/2019/02/04/chrome-js-reversing/ (дата обращения: 01.12.2021).
10. Горячев С.Н. Применение системного анализа для совершенствования методологии управления защитой информации. Применение современных информационных технологий в служебно-боевой деятельности: Материалы XIV Межвузовской научно-практической конференции, Пермь, 15 апреля 2020 года. Пермь: Федеральное государственное казенное военное образовательное учреждение высшего образования «Пермский военный институт войск национальной гвардии Российской Федерации», 2020. – 101 с. URL: https://www.elibrary.ru/item.asp?id=42793953&selid=42794079.
11. Макарова Ольга С., Поршнев Сергей В. Оценивание вероятностей компьютерных атак на основе метода анализа иерархий с динамическими приоритетами и предпочтениями. Безопасность информационных технологий, [S.l.], т. 27, № 1, с. 6–18, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.1.01.
12. Чеботарев Сергей В. О распределении сумм случайных величин с инвариантными связями и их моделировании. Журнал СФУ. Математика и физика. 2019, № 5, с. 628–636. URL: https://cyberleninka.ru/article/n/on-distribution-of-sums-of-random-variables-with-invariant-links-and-their-modeling (дата обращения: 03.12.2021).
13. Макарова Ольга С.; Поршнев Сергей В. Определение параметров, влияющих на возможность реализации компьютерной атаки нарушителем. Безопасность информационных технологий, [S.l.], т. 28, № 2, с. 6–20, 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.01.

REFERENCES:

[1] Smirnov V.M., Kiselev S.A. Malware as a threat to IAB Shape * MERGEFORMAT. Evraziiskii Soiuz Uchenykh 2020, no. 3-1 (72), p. 43–44. URL: https://cyberleninka.ru/article/n/vredonosnye-programmy-kak-opasnost-ovd-shape-mergeformat (accessed: 01.12.2021) (in Russian).
[2] Goldobina A.S., Isaeva YU.A., Selifanov V.V., Klimova A.M., Zenkin P.S. Building an adaptive three-level model of processes for managing the information protection system of critical information infrastructure

objects. Doklady TUSUR. 2018, no. 4, p. 51–58. URL: https://cyberleninka.ru/article/n/postroenie-adaptivnoy-trehurovnevoy-modeli-protsessov-upravleniya-sistemoy-zaschity-informatsii-obektov-kriticheskoy (accessed: 01.12.2021) (in Russian).

[3] Babenko A.A., Kozunova S.S. Information security management model in state information systems. NBI-technologies. 2018, no. 4, p. 16–22. URL: https://cyberleninka.ru/article/n/model-upravleniya-zaschitoy-informatsii-v-gosudarstvennyh-informatsionnyh-sistemah (accessed: 01.12.2021) (in Russian).

[4] Backih A.V., Drovnikova I.G. Model and algorithm for assessing the efficiency of functioning of the access control subsystem of the information protection system against unauthorized access in automated systems of the internal affairs bodies. Vestnik VI MVD Rossii. 2021, no. 2, p. 34–45. URL: https://cyberleninka.ru/article/n/model-i-algoritm-otsenki-effektivnosti-funktsionirovaniya-podsistemy-upravleniya-dostupom-sistemy-zaschity-informatsii-ot (accessed: 01.12.2021) (in Russian).

[5] Backih A.V. Simulation model of the functioning process of the modified access control subsystem of the information protection system against unauthorized access in the CPN TOOLS program environmentdostupa v programmnom okruzhenii CPN TOOLS. Vestnik VI MVD Rossii. 2020, no. 3, p. 96–106. URL: https://cyberleninka.ru/article/n/imitatsionnaya-model-protsessa-funktsionirovaniya-modifitsirovannoy-podsistemy-upravleniya-dostupom-sistemy-zaschity-informatsii-ot (accessed: 01.12.2021) (in Russian).

[6] Antonov A.V. System analysis: textbook. for universities.Antonov A.V. M.: Nauka i tekhnologii, 2008. – 177 p. (in Russian).

[7] Kurosh A.G. Kurs vysshej algebry. A.G. Kurosh. SPb.: Lan', 2006. – 432 s. (in Russian).

[8] Smirnov V.M., TSygankova IA.V., Nesterov I.A. State and trends of network security. Evraziiskii Soiuz Uchenykh. 2019, no. 9-2 (66), p. 42–43. URL: https://cyberleninka.ru/article/n/sostoyanie-i-trendy-setevoy-bezopasnosti (accessed: 30.11.2021) (in Russian).

[9] Virus-shifroval'shchik. xakep.ru. URL: https://xakep.ru/2019/02/04/chrome-js-reversing/ (accessed: 01.12.2021) (in Russian).

[10] Goryachev S.N. Application of system analysis to improve information security management methodology. Primenenie sovremennyh informacionnyh tekhnologij v sluzhebno-boevoj deyatel'nosti: Materialy XIV Mezhvuzovskoj nauchno-prakticheskoj konferencii, Perm', 15 aprelya 2020 goda. Perm': Federal'noe gosudarstvennoe kazennoe voennoe obrazovatel'noe uchrezhdenie vysshego obrazovaniya «Permskij voennyj institut vojsk nacional'noj gvardii Rossijskoj Federacii», 2020. – 101 s. URL: https://www.elibrary.ru/item.asp?id=42793953&selid=42794079 (accessed: 01.12.2021) (in Russian).

[11] Makarova Olga S., Porshnev Sergey V. Assessment of probabilities of computer attacks based on the method of analysis of hierarchies with dynamic priorities and preferences. IT Security (Russia), [S.l.], vol. 27, no. 1, p. 6–18, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.1.01.

[12] Chebotarev Sergey V. On distribution of sums of random variables with invariant links and their modeling. ZHurnal SFU. Matematika i fizika. 2019, no. 5, p. 628–636. URL: https://cyberleninka.ru/article/n/on-distribution-of-sums-of-random-variables-with-invariant-links-and-their-modeling (accessed: 01.12.2021) (in Russian).

[13] Makarova Ol'ga S., Porshnev Sergej V. Determination of parameters affecting the possibility of implementing a computer attack by an violator. IT Security (Russia), [S.l.], vol. 28, no. 2, p. 6–20, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.2.01.

Поступила в редакцию – 20 декабря 2021 г. Окончательный вариант – 28 февраля 2022 г.
Received – December 20, 2021. The final version – February 28, 2022.

Светлана А. Голуб[1], Игорь Ю. Коркин[2]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: glb.svtln@gmail.com, https://orcid.org/0000-0002-2395-0661
[2]e-mail: igor.korkin@gmail.com, https://orcid.org/0000-0001-7640-2792

АНАЛИЗ БЕЗОПАСНОСТИ ПОДСИСТЕМ ЛОКАЛЬНОЙ АУТЕНТИФИКАЦИИ ОС СЕМЕЙСТВ WINDOWS И LINUX

DOI: http://dx.doi.org/10.26583/bit.2022.1.06

Аннотация. Работа посвящена одному из ключевых вопросов безопасности современных операционных систем Windows и Linux – анализу защищённости парольной информации пользователей. Для операционной системы Windows проводится анализ процессов локальной аутентификации и аутентификации с использованием контроллера домена. Для демонстрации атак на подсистему аутентификации рассмотрено программное средство Mimikatz (Франция), позволяющее извлекать парольную информацию из памяти процесса LSASS. Представлен анализ штатных средств ОС Windows для защиты памяти процессов: Security Reference Monitor, Protected Process Light и Virtualization-Based Security. Нарушитель с помощью драйвера ядра может получить доступ к парольной информации пользователя в обход штатных средств защиты. Для Linux-подобных систем представлен результат аналогичного анализа безопасности подсистем локальной аутентификации. Показано, что в модуле GNOME памяти процесса gnome-keyring-daemon можно обнаружить пароли пользователей в открытом виде, которые нарушитель может извлечь, используя привилегии прикладной программы пользовательского уровня. Данная проблема остаётся актуальной для многих современных ОС Linux на базе дистрибутива компании RedHat, таких как CentOS, Ubuntu, GNU/Linux Rolling. Для устранения описанной проблемы исследователями были разработаны программные средства для поиска и удаления паролей из памяти: MimiPenguin (США) и Mimipy (США). Сравнительный анализ этих средств показал их недостатки: средства не могут осуществлять поиск и удаление паролей, состоящих из символов Юникод (Unicode) кодировки, а также имеют медленную скорость работы. Предлагаемое в работе программное средство защиты MimiDove расширяет возможности имеющихся средств и позволяет находить и удалять из памяти пароли, содержащие символы из наборов ASCII и Unicode, затрачивая значительно меньше времени.

Ключевые слова: извлечение данных пользователя, пароли в памяти, ASCII и Unicode символы, безопасность операционных систем, gnome-keyring-daemon, LSASS, Mimikatz.
Для цитирования: ГОЛУБ, Светлана А.; КОРКИН, Игорь Ю. АНАЛИЗ БЕЗОПАСНОСТИ ПОДСИСТЕМ ЛОКАЛЬНОЙ АУТЕНТИФИКАЦИИ ОС СЕМЕЙСТВ WINDOWS И LINUX. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 57–69, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1402. DOI: http://dx.doi.org/10.26583/bit.2022.1.06.

Svetlana A. Golub[1], Igor Y. Korkin[2]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: glb.svtln@gmail.com, https://orcid.org/0000-0002-2395-0661
[2]e-mail: igor.korkin@gmail.com, https://orcid.org/0000-0001-7640-2792

An Analysis of Local Security Authority Subsystem Services for Windows and Linux

DOI: http://dx.doi.org/10.26583/bit.2022.1.06

Abstract. The paper is devoted to the security analysis of authority subsystem services for Windows and Linux operating systems. The paper provides security analysis for both local and network-based authentication in Windows. The Mimikatz (France) will be presented to demonstrate attacks on the authentication subsystem. Mimikatz is a software tool that can extract users' credentials and password information from the memory of the LSASS process. To prevent such attacks on process memory

Windows OS includes several security mechanisms: Security Reference Monitor, Protected Process Light, and Virtualization-Based Security. However, attackers can bypass these mechanisms to get illegal access to the process memory and steal users' credentials. A similar analysis of the local authority subsystem for Linux OSes shows that gnome-keyring-daemon stores the users' passwords in plain text. As a result, attackers can easily extract this sensitive information using memory forensics techniques via user-mode applications. Several modern Linux Distributions based on Red Hat Enterprise Linux (RHEL) still have this security issue: CentOS, Ubuntu, GNU/ Linux Rolling. Experts have developed software tools to locate and remove passwords from the memory to tackle this security challenge: MimiPenguin (USA) and Mimipy (USA). Comparison analysis of these tools reveals their drawbacks: these security tools cannot locate passwords with Unicode characters, and these tools have low speed. The proposed security solution called MimiDove is designed to solve both these issues. MimiDove expands features of MimiPenguin and Mimipy by locating and deleting passwords with ASCII and Unicode characters. MimiDove is faster than MimiPenguin and Mimipy.

Keywords: extraction credentials, passwords in memory, ASCII and Unicode passwords, operating system security, gnome-keyring-daemon, LSASS, Mimikatz.

For citation: GOLUB, Svetlana A.; KORKIN, Igor Y. An Analysis of Local Security Authority Subsystem Services for Windows and Linux. IT Security (Russia), [S.l.], v. 29, n. 1, p. 57–69, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1402. DOI: http://dx.doi.org/10.26583/bit.2022.1.06.

Введение

Операционные системы семейств Windows и Linux являются доминирующими на рынках персональных и серверных компьютерных систем. Согласно опубликованной статистике компании Майкрософт, операционная система Windows 10 обеспечивает работу более 1 миллиарда персональных устройство в 200 странах мира. Linux занимает менее 2% объёма рынка персональных компьютеров, однако более 96% всех веб-серверов работают под управлением Linux.

Обеспечение безопасности парольной информации пользователей является первостепенной задачей в любой информационной инфраструктуре. В настоящее время существует множество атак, позволяющих получить несанкционированный доступ к парольным данным пользователей. Проведение успешных атак на подсистемы локальной аутентификации позволяет нарушителям получить несанкционированный доступ к учётным данным пользователя. Программные средства для эксплуатации уязвимостей в подсистеме аутентификации использовались такими известными хакерскими группировками, как APT28, APT39, Carbanak, Axiom и многими другими [1]. Компании, которые подверглись их атакам, понесли большие материальные и репутационные потери.

В работе проводится анализ безопасности подсистем аутентификации в ОС Windows и Linux. Windows занимает большую часть рынка операционных систем для персональных компьютеров и атаки на эту ОС наиболее распространены. В то же время Linux-подобные системы сейчас являются основой корпоративной инфраструктуры. Серверы крупных компаний работают под управлением ОС Linux. Для исследования была выбрана операционная система Community Enterprise Operating System (CentOS), основанная на ОС Red Hat Enterprise Linux, и используемая при развертывании критически важных приложений на мировых биржах, в финансовых учреждениях и в ведущих телекоммуникационных компаниях.

Исследователями было обнаружено, что пароли пользователей хранятся в открытом виде длительное время в памяти сервисов ОС Linux, предназначенных для безопасного хранения информации. Эта уязвимость была подтверждена и зарегистрирована как CVE-2018-20781 [2]. Нарушители могут извлечь содержимое паролей пользователей путём чтения памяти соответствующего процесса. Некоторые

процессы в дистрибутивах ОС Linux последних версий до сих пор остаются уязвимыми к атакам, позволяющим извлекать учётные данные из памяти.

В работе проводится анализ атак на подсистемы локальной аутентификации в ОС Windows и ОС Linux и предлагаются способы им противодействия. Описывается разработанное программное средство для удаления парольной информации, содержащей как ASCII, так и Unicode символы из памяти ОС Linux, имеющее конкурентные преимущества.

1. Анализ безопасности подсистемы локальной аутентификации ОС Windows: современные атаки и защита от них

Все широко используемые современные операционные системы являются многопользовательскими. Для того, чтобы получить доступ к учётной записи, пользователю необходимо пройти процесс аутентификации, который отвечает за подтверждение подлинности пользователя для дальнейшей авторизации в системе. Данный процесс входит в подсистему локальной аутентификации операционной системы.

В ОС Windows учётные данные локальных пользователей хранятся в базе данных Security Account Manager (SAM) в виде хеш-кода NTLM [3]. Для его вычисления при локальной аутентификации используется хеш-функция MD4. Хеш-коды вычисляются единожды за сессию без добавления «соли» и впоследствии не меняются. Иерархическая база данных SAM расположена в ключе реестра HKEY_LOCAL_MACHINE\SAM\SAM и по умолчанию недоступна ни обычным пользователям, ни администраторам. В ветке реестра каждого пользователя можно найти информацию об учётной записи, домашней директории, попытках входа, хеш-код LM (если хеширование LM не отключено) и хеш-код NTLM.

За реализацию локальной политики безопасности отвечает сервис проверки подлинности локальной системы безопасности (Local Security Authority Subsystem Service, LSASS) [4, с. 155]. После того как пользователь вводит свои учетные данные, вычисляется хеш-код NTLM. Для его проверки служба WinLogon загружает графическую динамическую библиотеку GINA для интерактивной идентификации и аутентификации, которая передаёт их в функцию LsaLogonUser [5]. Сервис проверки подлинности LSASS использует пакет аутентификации MSV1_0 для обработки введённых данных. Пакет MSV1_0 обращается к базе учётных данных SAM, чтобы проверить подлинность пользователя, а затем возвращает результат попытки входа в систему сервису проверки подлинности LSASS. Процесс LSASS.exe сохраняет в памяти хеш-коды NTLM паролей пользователей с активными сеансами для реализации возможности единого входа (Single Sign-On, SSO), который позволяет пользователю получать доступ к различным службам, не проходя повторную аутентификацию. Процесс локальной аутентификации представлен на рис. 1.

В доменных сетях может использоваться другой механизм аутентификации. Доменная сеть позволяет централизованно управлять компьютерами, подключёнными к одной сети. В домене Windows вся информация об учетных записях пользователей, компьютерах, подключенных устройствах и политиках безопасности записана в центральной базе данных, расположенной на одном или нескольких главных компьютерах, которые называются контроллерами домена. Эта информация об учетных записях пользователей может храниться в локальной базе учётных данных SAM, либо удалённо, с использованием службы Active Directory и контроллера домена [6].

Аутентификация в домене Windows осуществляется с помощью контроллеров домена.

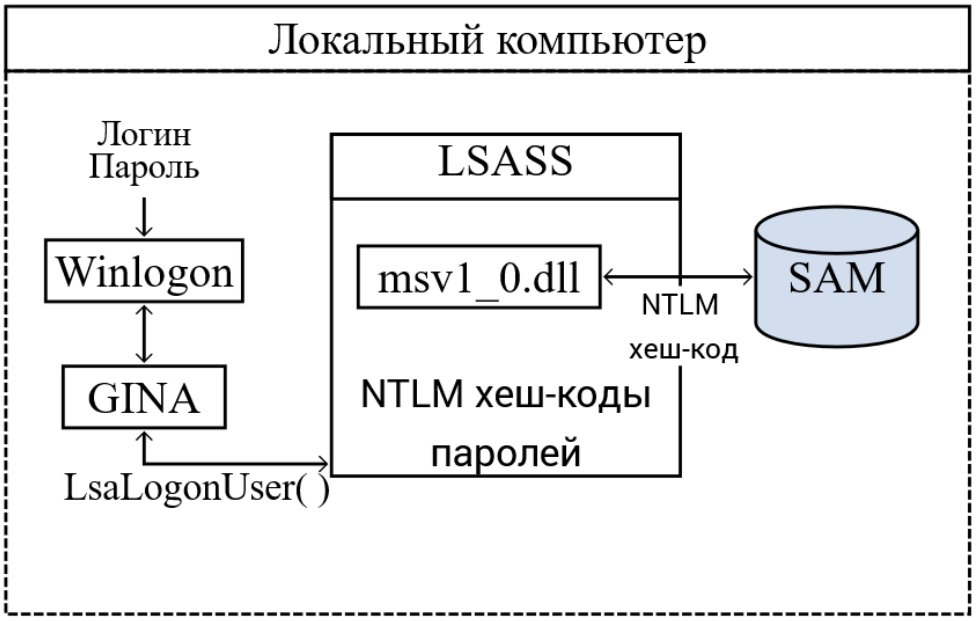


Рис. 1. Процесс локальной аутентификации
Fig. 1. The scheme of the local authentication

Аутентификация в домене также возможна с помощью протокола NTLM. Для этого используется пакет MSV, он делится на две части: одна часть MSV1_0 осуществляет преобразование открытого пароля пользователя в хеш-код пароля LM и/или хеш-код пароля NTLM, затем хеш-код передаётся в службу NetLogon. На следующем этапе служба NetLogon вызывает вторую часть пакета MSV, расположенную на контроллере домена, и которая, в свою очередь, осуществляет проверку хеш-кода пароля с помощью базы учётных записей контроллера домена SAM. Результат проверки через первую часть пакета MSV на локальном компьютере передаётся сервису проверки подлинности LSASS, который принимает решение, давать ли пользователю доступ к системе. Процесс аутентификации пользователя в домене представлен на рис. 2.

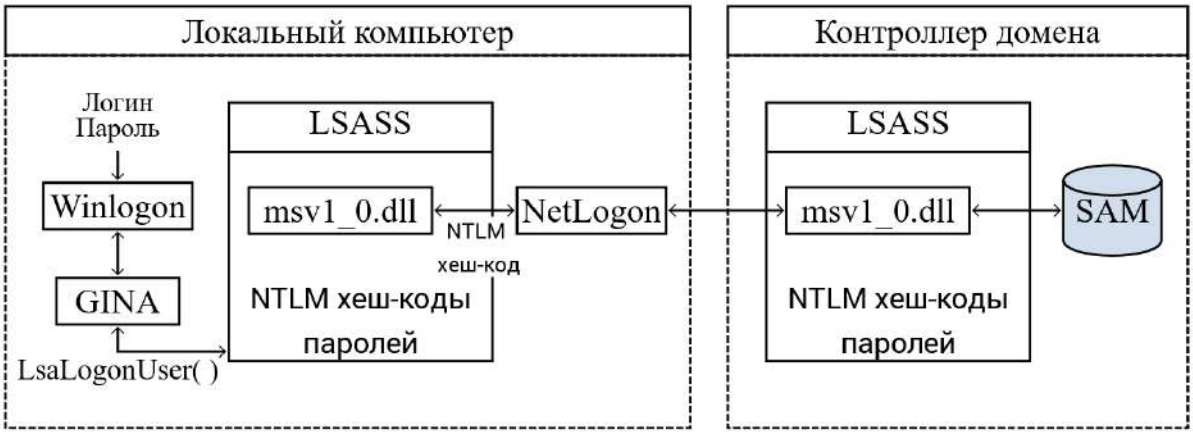


Рис. 2. Процесс аутентификации в домене
Fig. 2. The scheme of domain-based authentication

1.1. Анализ программного средства Mimikatz для извлечения парольной информации из памяти процессов Windows

Французский исследователь Бенджамин Делпи разработал утилиту Mimikatz для ОС Windows, которая с помощью драйвера позволяет извлекать следующую парольную информацию: пароли пользователя в открытом виде, хеш-коды NTLM, билеты Kerberos, сертификаты SSL и ключи шифрования [7]. Сама по себе программа не является вредоносной, но может быть использована нарушителями для осуществления следующих атак: «pass-the-ticket» [6] и «pass-the-hash» [8].

1.1.1. Атака «pass-the-hash»

В случае, если в операционной системе для локальной аутентификации используется протокол LM или NTLM, пароли пользователей передаются по каналу в виде хеш-кодов. Для восстановления пароля из хеш-кода нарушителю требуется проведения перебора значений хеш-функции, что требует значительных временных и вычислительных ресурсов. Соответственно на этапе ответа в схеме аутентификации «запрос-ответ» предоставляются хеш-коды паролей без использования «соли». Таким образом, нарушитель может использовать для несанкционированного доступа только значение хеш-кода пароля без необходимости получения пароля пользователя.

Программа Mimikatz может извлечь хеш-коды NTLM с помощью дампа памяти процесса LSASS.exe. Для этого Mimikatz получает привилегии отладки, благодаря которым может получить доступ к процессам, запускаемым от системных учётных записей. По умолчанию в локальной политике безопасности привилегия отладки выдаётся группе BUILTIN\Administrators. Это значит, что при выставленном идентификаторе безопасности (SID) этой группы можно получить данную привилегию. Таким образом, Mimikatz получает доступ к процессу LSASS.exe, следовательно, и к хеш-кодам NTLM. Имея хеш-код NTLM, можно напрямую пройти аутентификацию в системе, что показано на рис. 3.

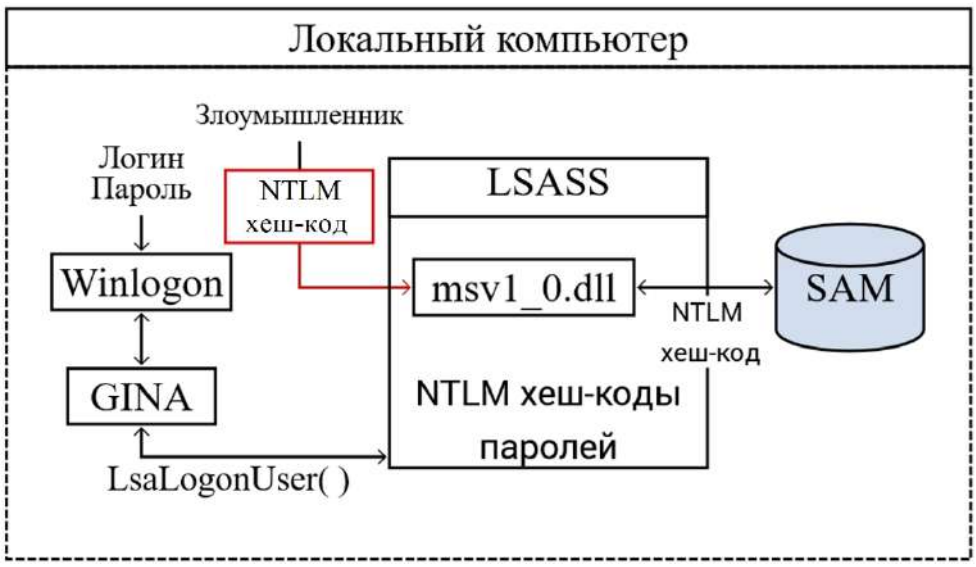


Рис. 3. Атака «pass-the-hash»
Fig. 3. "Pass-The-Hash" Attack

1.1.2. Атака «pass-the-ticket»

В модели клиент-сервер взаимная аутентификация осуществляется с помощью протокола Kerberos, который предполагает наличие третьей независимой стороны.

Посредником между клиентом и сервером выступает доверенный центр аутентификации – центр распределения ключей (Key Distribution Center, KDC), который хранит информацию об учётных записях всех клиентов сети, в частности, долговременные ключи, которые создаются на основе пароля пользователя. Центр распределения ключей Kerberos интегрирован с другими службами безопасности Windows Server, работающими на контроллере домена. KDC использует службу Active Directory в качестве базы данных учетных записей пользователей.

Введённый пользователем пароль преобразуется в хеш-код NTLM и, с использованием библиотеки Kerberos, передаётся в контроллер домена для проверки подлинности пользователя. Процесс аутентификации по протоколу Kerberos представлен на рис. 4.

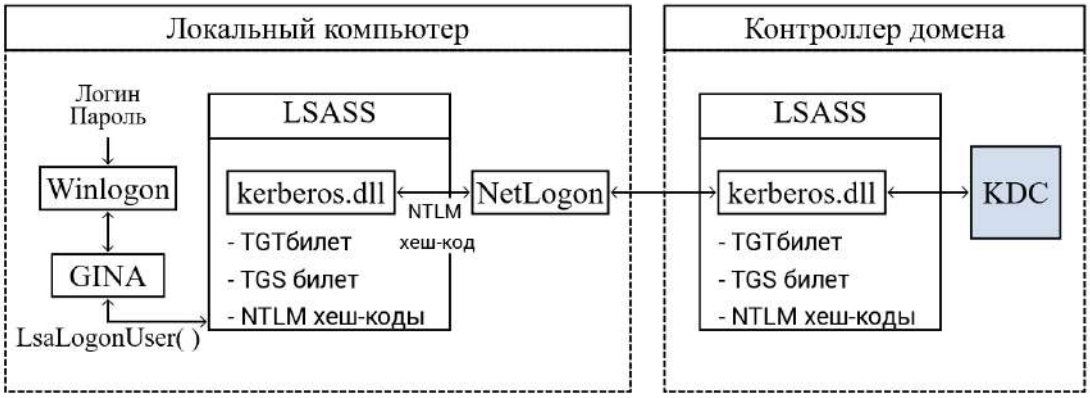


Рис. 4. Схема процесса аутентификации с использованием протокола Kerberos
Fig. 4. The Kerberos authentication protocol scheme

Для получения доступа к какой-либо службе клиенту необходимо осуществить первичную аутентификацию. На первом этапе клиент должен предоставить хеш-код NTLM для пароля, своё имя и зашифрованную временную метку. Если они подлинные, KDC выдаёт пользователю зашифрованный билет – Ticket Granting Ticket (TGT) с ограниченным временем жизни и сеансовый ключ. TGT билет включает в себя имя пользователя, запрашивающего билет, сгенерированный сессионный ключ пользователя, время жизни билета и сертификат атрибута привилегий (Privilege Attribute Certificate, PAC), который определяет права пользователя в системе. Ключом для шифрования является хеш-код NTLM для пароля, а алгоритм шифрования, может быть, одним из следующих: RC4, AES128, AES256. В дальнейшем, предъявляя TGT билет, идентификатор сервиса и зашифрованные сеансовым ключом временную метку и имя, клиент может получить от KDC зашифрованный Ticket Granting Service (TGS) для доступа к конкретному сервису. TGS состоит из сеансового ключа сервиса, имени пользователя, запрашивающего доступ, времени жизни билета и список привилегий PAC пользователя относительно запрашиваемого сервиса. Ключом шифрования является хеш-код NTLM владельца сервиса. Такой же билет доверенный центр выдаёт и сервису, посредством чего достигается взаимная аутентификация. Оба билета имеют ограниченный срок жизни. Все билеты сохраняются в памяти процесса LSASS для осуществления дальнейшего доступа к сервисам. Упрощённый процесс получения билета TGS представлен на рис. 5.

Благодаря программе Mimikatz можно несколькими способами получить доступ к сервису, не зная паролей пользователя. Такая атака называется «pass-the-ticket». Для получения TGT пользователь отправляет свой ключ, который является хеш-кодом пароля. Нарушитель может получить хеш-код NTLM и, используя его, пройти дальнейшую

аутентификацию. Нарушитель может подменить все TGT для администратора домена. После чего KDC предоставляет нарушителю TGS, и он получает доступ к сервису, как показано на рис. 6.

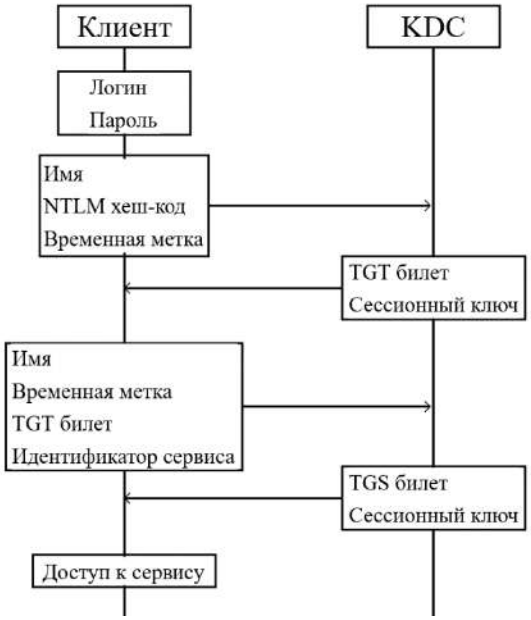


Рис. 5. Процесс получения билета TGS
Fig. 5. The scheme of gathering TGS tickets

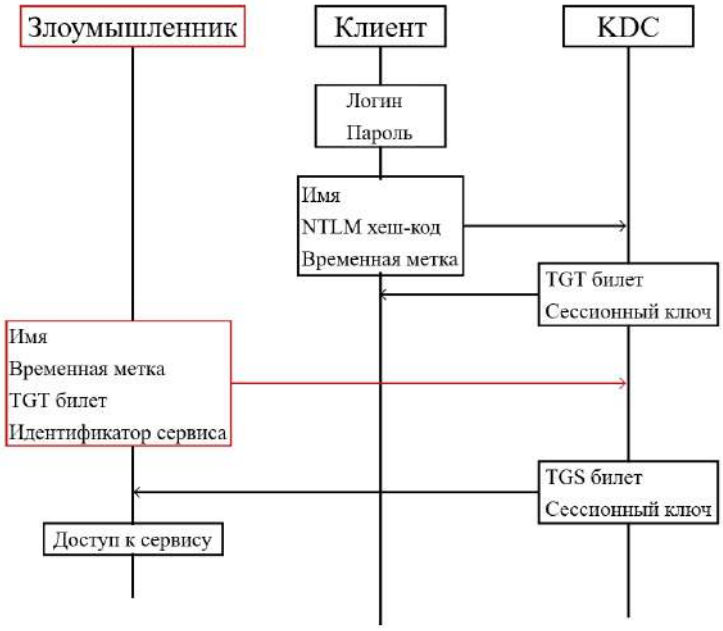


Рис. 6. Атака «pass-the-ticket» через TGT
Fig. 6. The scheme of «pass-the-ticket» attack via TGT

По такому же принципу нарушитель может получить и TGS. Этот вариант аутентификации представлен на рис. 7.

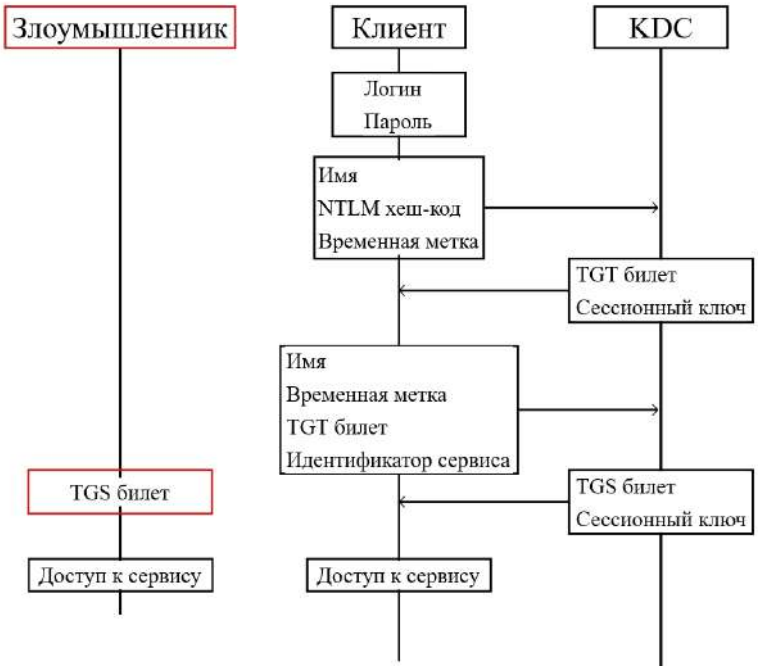


Рис. 7. Атака «pass-the-ticket» через TGS
Fig. 7. The scheme of «pass-the-ticket» attack via TGS

1.2. Анализ встроенных механизмов защиты памяти процессов на примере LSASS

Для защиты парольной информации пользователя, хранящейся в памяти процесса LSASS, от несанкционированного доступа, разработчики Windows реализовали ряд средств защиты: SRM, PPL, VBS. Проведем анализ этих средств и рассмотрим примеры атак, направленных на противодействие этим средствам защиты.

1.2.1. Монитор безопасности (Security Reference Monitor, SRM)

Штатный механизм безопасности ОС Windows, называемый монитором безопасности (Security Reference Monitor, SRM), обеспечивает контроль доступа к памяти программ на основе данных токена и дескриптора безопасности. Данный механизм позволяет предотвратить доступ к памяти программ, работающих с более высокими привилегиями, со стороны менее привилегированных программ. Однако, если вредоносная программа имеет привилегии отладки SeDebugPrivilege, то монитор безопасности всегда предоставляет такой программе полный доступ к памяти других программ без каких-либо дополнительных проверок безопасности, что может быть использовано нарушителем.

1.2.2. Защищённые процессы (Protected Process Light, PPL)

Для предотвращения такого несанкционированного доступа и для защиты мультимедийного контента от копирования (Digital Rights Management), памяти процесса LSASS.EXE и антивирусных средств защиты (Early Launch AntiMalware, ELAM) в ОС Windows был добавлен новый механизм для защиты памяти процессов, называемый «Защищённые процессы» (Protected Process Light, PPL). Процессы LSASS.EXE и Windows Defender запускаются как «PPL-защищённые». Процессы, имеющие специальную цифровую подпись, загружаются как «PPL-защищённые», процессы без подписи загружаются как обычные или «PPL-незащищённые». Механизм PPL блокирует любой доступ к памяти «PPL-защищённых» процессов со стороны «PPL-незащищённых», даже если они были запущены с привилегиями отладки. Информация о том, является ли

работающий процесс защищённым, хранится в поле Protection типа PS_PROTECTION, которое было добавлено в структуру EPROCESS. При каждом запросе на получение доступа к процессу с помощью вызова функций CreateProcess() или OpenProcess() ядро Windows производит чтение содержимого поля Protection.

Механизм PPL, в свою очередь, также уязвим и может быть отключён. Нарушитель с помощью драйвера может изменить значение поля Protection: либо понизить привилегии для «PPL-защищённого» процесса, либо наоборот повысить привилегии для вредоносного «PPL-незащищённого» процесса. В результате такой манипуляции доступ к памяти «PPL-защищённого» процесса будет предоставлен без срабатывания штатных средств самозащиты ядра, таких как Kernel Patch Protection (KPP, PatchGuard).

При включённом механизме PPL процесс LSASS запускается как «PPL-защищённый». С помощью драйвера Mimikatz может переписать нулями поле Protection для процесса LSASS, в результате LSASS процесс станет «PPL-незащищённым» и доступ к нему можно будет получить по описанной выше схеме.

1.2.3. Защита памяти с использованием технологии аппаратной виртуализации (Virtualization Based Security, VBS)

Для компенсации недостатков механизмов PPL и SRM компания Microsoft выпустила новый механизм для защиты памяти процесса LSASS и пользовательских учётных данных. Благодаря гипервизору на базе технологии аппаратной виртуализации Hyper-V стало возможным использовать новый режим работы Virtual Secure Mode (VSM), в результате которого часть ядра и защищаемые прикладные программы стали выполняться изолированно от основного ядра и других программ. Таким образом, стало возможным обеспечить защиту памяти с использованием технологии аппаратной виртуализации (Virtualization Based Security, VBS). В настоящее время режим VSM поддерживает два уровня доверия Virtual Trust Levels (VTLs) [9]. На нулевом уровне VTL0 (normal mode) происходит выполнение большинства прикладных программ и основной части ядра ОС Windows; в то время как первый уровень VTL1 (secure mode) предназначен для работы программ и драйверов с повышенными требованиями по безопасности. Для запуска на уровне VTL1 программа должна быть подписана специальным цифровым сертификатом, что исключает запуск вредоносных программ в режиме VTL1. Режим VSM гарантирует отсутствие доступа драйверов и программ из VTL0 в VTL1.

Программы в VTL1 выполняются в изолированном пользовательском режиме (Isolated User Mode, UIM) и называются доверенными приложениями или трастлетами (trustlet, trusted application). Драйвера в VTL1 работают в защищённом режиме ядра (secure kernel).

При включённом режиме VSM программа LSASS.EXE (LSAISO.EXE) работает как трастлет, то есть выполняется как процесс изолированного режима. Учётные данные пользователей хранятся в памяти процесса LSAISO.exe, который является изолированным и взаимодействует с LSASS с помощью механизма удалённого вызова процедур. VSM гарантирует отсутствие доступа к памяти процесса LSAISO.exe со стороны прикладных программ и драйверов, запущенных в VTL0.

Описанный механизм защиты памяти с использованием технологии аппаратной виртуализации доступен в Windows ОС начиная с версии 10 только для редакций Enterprise, в то время как другие версии операционной системы всё ещё остаются уязвимыми для описанных атак. Для защиты памяти процесса LSASS, а также для предотвращения несанкционированного повышения PPL для вредоносных процессов возможно использовать альтернативное решение на базе гипервизора MemoryRanger [10].

2. Анализ безопасности подсистемы локальной аутентификации ОС Linux: современные атаки и защита от них

Операционные системы на базе ядра Linux также подвержены аналогичной атаке на подсистему локальной аутентификации: вредоносные процессы, запущенные с необходимыми привилегиями, могут получить несанкционированный доступ к памяти других работающих процессов для чтения и перезаписи обрабатываемых данных.

В табл. 1 представлен список процессов и данные пользователя, которые могут быть извлечены.

Таблица 1. Список процессов и соответствующая парольно-адресная информация пользователя

Linux-процесс	Парольно-адресная информация пользователя в памяти процесса
gnome-keyring-daemon	• ключи и сертификаты; • имена и пароли текущих пользователей.
apache2	• пароли аутентифицированных пользователей для доступа к веб-ресурсам.
vsftpd	• информация об активных FTP подключениях клиента;
sshd	• информация об активных SSH подключениях.

Исследователь Seong-Joong Kim [11] обнаружил, что в GNOME Keyring версии 3.18.3 пароли всех активных пользователей находятся в открытом виде в памяти процесса gnome-keyring-daemon. Причиной этому является отсутствие вызова функций для перезаписи содержимого памяти из-за особенностей работы компиляторов и оптимизаторов [11]. Эксперты по безопасности разработали ряд программных средств для извлечения и удаления парольно-адресной информации пользователя из памяти процессов. Далее будет осуществлён анализ двух таких средств: MimiPenguin и MimiPy.

2.1. Анализ работы средства MimiPenguin по извлечению парольной информации

Исследователь Hunter J. Gregal из США разработал программное средство MimiPenguin [12] для поиска паролей активных пользователей в памяти процесса gnome-keyring-daemon. Программа MimiPenguin извлекает из памяти пароли активных учётных записей в открытом виде. Для проверки извлечённых паролей MimiPenguin осуществляет их хеширование и сравнение со значениями хеш-кодов паролей из файла /etc/shadow.

MimiPenguin имеет следующие недостатки:

- поддержка поиска паролей только из печатных ASCII символов, отсутствие возможностей поиска паролей из Unicode символов;
- отсутствие функций перезаписи найденной парольной информации;
- низкая скорость работы.

2.2. Анализ работы средства Mimipy по извлечению парольной информации

Исследователь Nicolas Verdier из США на основе средства MimiPenguin разработал программное средство Mimipy [13]. Он добавил возможность перезаписи найденных в памяти паролей.

Программа Mimipy имеет следующие недостатки:

- поддержка поиска паролей только из печатных ASCII символов, отсутствие возможностей поиска паролей из Unicode символов;
- низкая скорость работы.

3. Авторское программное средство MimiDove исключает недостатки конкурентов по защите парольной информации

Для противодействия угрозам утечки парольной информации необходимо иметь возможность перезаписи найденных в памяти паролей вне зависимости от алфавита их символов. На основе программы MimiPenguin было разработано программное средство MimiDove [14].

3.1. Расширение словаря паролей

Linux-подобные операционные системы широко используются в различных странах, и в общем случае пароли пользователя могут содержать символы национальных языков, которые могут быть представлены с использованием кодировок ASCII и Unicode. В отличие от существующих программных средств MimiPenguin и MimiPy, где используется поиск только по печатным символам ASCII, в данной работе поиск осуществляется с учётом всех возможных символов, за исключением нулевого символа. Нулевой байт является индикатором конца предыдущей строки и начала новой со следующего байта.

3.2. Ускорение алгоритма поиска

Для ускорения поиска проведён анализ памяти процессов gnome-keyring-daemon разных пользователей. Это позволило определить расположение паролей. Они находятся в одной из последних областей памяти среди тех, что обозначены в файлах /proc/PID/maps.

Файл включает в себя следующую информацию о каждом блоке памяти процесса:

- адрес начала и конца блока в адресном пространстве процесса;
- права доступа к блоку памяти (read, write, execute);
- смещение, индексный дескриптор inode файла и имя файла, если область памяти была отображена из другого файла (процесса) с помощью утилиты mmap;
- основной и второстепенный номера устройств, если область памяти была отображена из специального файла устройства.

В процессе gnome-keyring-daemon учётные данные во время обработки находятся в стек-памяти. Причиной нахождения паролей в памяти процесса является неправильная работа со стеком во время обработки чувствительных данных в процессе, отвечающем за аутентификацию gnome-keyring-daemon. Программное средство MimiDove с помощью файла /proc/<PID>/maps вычисляет относительные адреса областей памяти процессов, на которые был отображен стек родительских процессов. Данный приём позволил значительно сократить время поиска паролей.

3.3. Удаление паролей из памяти процессов

Парольно–адресная информация пользователей не должна храниться в памяти процессов в открытом виде. Общим решением этой задачи является исправление кода уязвимых программных продуктов: корректная работа с указателями, использование безопасных функций. Но зачастую этот процесс бывает длительным, и не всегда существует возможность оперативно внести изменения в исходный текст программы и установить обновленное программное обеспечение. В качестве частного решения (adhoc) можно рассмотреть возможность автоматического удаления остаточной информации из памяти процессов.

В программном средстве MimiPenguin была реализована возможность удаления паролей из памяти процессов: при этом найденный пароль можно перезаписывать как нулевыми символами, так и ненулевыми символами, для сокрытия факта очистки паролей.

3.4. Сравнение существующих средств по поиску и перезаписи паролей

Разработанное программное средство MimiDove имеет следующие конкурентные преимущества:

- возможность поиска и перезаписи паролей, состоящих из ASCII и Unicode символов;
- высокая скорость работы.

Сравнительные характеристики программ приведены в табл. 2.

Таблица 2. Сравнительные характеристики программ

Название программы	Среднее время работы, сек.	Возможность поиска паролей из символов		Возможность перезаписи паролей из символов	
		ASCII	Unicode	ASCII	Unicode
MimiPenguin	90	+	–	–	–
Mimipy	50	+	–	+	–
MimiDove	2	**+**	**+**	**+**	**+**

Заключение

В настоящей работе проведён анализ механизмов работы подсистем аутентификации в современных операционных системах Windows и Linux на примере техник извлечения из памяти процессов парольно-адресной информации. Определены места хранения парольных данных пользователя, рассмотрены возможные атаки с целью получения доступа к парольным данным пользователей и возможные способы защиты от этих атак. Проведён анализ средств по извлечению парольной- информации пользователя: Mimikatz (Франция), MimiPenguin (США) и Mimipy (США). Рассмотрено влияние расширения паролей на работу программ для извлечения учётных данных.

Реализованное программное средство MimiDove позволяет находить и перезаписывать пароли из памяти процессов вне зависимости от используемого алфавита, что исключает несанкционированный доступ к парольной информации.

СПИСОК ЛИТЕРАТУРЫ:

1. OS Credential Dumping, MITRE ATT&CK, 2018. URL: https://attack.mitre.org/techniques/T1003/ (дата обращения: 20.01.2022).
2. CVE-2018-20781. MITRE, 2018. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20781 (дата обращения: 20.01.2022).
3. Du J., Li J. Analysis the Structure of SAM and Cracking Password Base on Windows Operating System. In: International Journal of Future Computer and Communication (IJFCC). 2016, vol. 5, no. 2, p. 112–115. DOI: https://doi.org/10.18178/ijfcc.2016.5.2.455.
4. Ligh M., Case A., Levy J., Walters. A. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Indianapolis, Indiana. John Wiley & Sons. 2014. – 912 p.
5. Bassil Y. Windows and Linux Operating Systems from a Security Perspective. Journal of Global Research in Computer Science. 2012, vol. 3, no. 2. URL: https://arxiv.org/ftp/arxiv/papers/1204/1204.0197.pdf (дата обращения: 20.01.2022).
6. Kotlaba L. Active Directory Kerberoasting Attack: Monitoring and Detection Techniques. In Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020). 2020, p. 432–439. DOI: https://doi.org/10.5220/0008955004320439.
7. Delpy B. Mimikatz. URL: https://github.com/gentilkiwi/mimikatz (дата обращения: 20.01.2022).
8. Dimov D., Tzonev Y. Pass-the-Hash: One of the Most Prevalent Yet Underrated Attacks for Credentials Theft and Reuse. In Proceedings of the 18th International Conference on Computer Systems and Technologies (CompSysTech'17). 2017, p. 149–154. DOI: https://doi.org/10.1145/3134302.3134338.
9. Isolated User Mode (IUM) Processes. URL: https://docs.microsoft.com/en-us/windows/win32/procthread/isolated-user-mode--ium--processes (дата обращения: 20.01.2022).

10. Korkin I. Protected Process Light is not Protected: MemoryRanger Fills the Gap Again. Systematic Approaches to Digital Forensic Engineering (SADFE) International Workshop in conjunction with the 42nd IEEE Symposium on Security and Privacy. 2021, p. 298–308. DOI: https://doi.org/10.1109/SPW53761.2021.00050.
11. Besson F., Dang A., Jensen T. Securing Compilation Against Memory Probing. In Proceedings of the 13th Workshop on Programming Languages and Analysis for Security (PLAS'18). 2018, p. 29–40. DOI: https://doi.org/10.1145/3264820.3264822.
12. Gregal H. Mimipenguin. URL: https://github.com/huntergregal/mimipenguin (дата обращения: 20.01.2022).
13. Verdier N. Mimipy. URL: https://github.com/n1nj4sec/mimipy (дата обращения: 20.01.2022).
14. Golub S. MimiDove. URL: https://github.com/SvetlanaGolub/MimiDove (дата обращения: 20.01.2022).

REFERENCES:

[1] OS Credential Dumping, MITRE ATT&CK, 2018. URL: https://attack.mitre.org/techniques/T1003/ (accessed: 20.01.2022).
[2] CVE-2018-20781. MITRE, 2018. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20781 (accessed: 20.01.2022).
[3] Du J., Li J. Analysis the Structure of SAM and Cracking Password Base on Windows Operating System. In: International Journal of Future Computer and Communication (IJFCC). 2016, vol. 5, no. 2, p. 112–115. DOI: https://doi.org/10.18178/ijfcc.2016.5.2.455.
[4] Ligh M., Case A., Levy J., Walters. A. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Indianapolis, Indiana. John Wiley & Sons. 2014. – 912 p.
[5] Bassil Y. Windows and Linux Operating Systems from a Security Perspective. Journal of Global Research in Computer Science. 2012, vol. 3, no. 2. URL: https://arxiv.org/ftp/arxiv/papers/1204/1204.0197.pdf (accessed: 20.01.2022).
[6] Kotlaba L. Active Directory Kerberoasting Attack: Monitoring and Detection Techniques. In Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020). 2020, p. 432–439. DOI: https://doi.org/10.5220/0008955004320439.
[7] Delpy B. Mimikatz. URL: https://github.com/gentilkiwi/mimikatz (accessed: 20.01.2022).
[8] Dimov D., Tzonev Y. Pass-the-Hash: One of the Most Prevalent Yet Underrated Attacks for Credentials Theft and Reuse. In Proceedings of the 18th International Conference on Computer Systems and Technologies (CompSysTech'17). 2017, p. 149–154. DOI: https://doi.org/10.1145/3134302.3134338.
[9] Isolated User Mode (IUM) Processes. URL: https://docs.microsoft.com/en-us/windows/win32/procthread/isolated-user-mode--ium--processes (accessed: 20.01.2022).
[10] Korkin I. Protected Process Light is not Protected: MemoryRanger Fills the Gap Again. Systematic Approaches to Digital Forensic Engineering (SADFE) International Workshop in conjunction with the 42nd IEEE Symposium on Security and Privacy. 2021, p. 298–308. DOI: https://doi.org/10.1109/SPW53761.2021.00050.
[11] Besson F., Dang A., Jensen T. Securing Compilation Against Memory Probing. In Proceedings of the 13th Workshop on Programming Languages and Analysis for Security (PLAS'18). 2018, p. 29–40. DOI: https://doi.org/10.1145/3264820.3264822.
[12] Gregal H. Mimipenguin. URL: https://github.com/huntergregal/mimipenguin (accessed: 20.01.2022).
[13] Verdier N. Mimipy. URL: https://github.com/n1nj4sec/mimipy (accessed: 20.01.2022).
[14] Golub S. MimiDove. URL: https://github.com/SvetlanaGolub/MimiDove (accessed: 20.01.2022).

Поступила в редакцию – 20 декабря 2021 г. Окончательный вариант – 13 февраля 2022.
Received – December 20, 2021. The final version – February 13, 2022.

Виктор С. Горбатов[1], Дмитрий А. Дятлов[2], Роман В. Наталичев[3]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733
[2]e-mail: DADyatlov@mephi.ru, https://orcid.org/0000-0001-9967-6366
[3]e-mail: r.natalichev2015@yandex.ru, https://orcid.org/0000-0002-8985-7144

ОБ УСТОЙЧИВОСТИ ЛОГИСТИЧЕСКИХ СТРУКТУР НА ОСНОВЕ СМАРТ-КОНТРАКТОВ

DOI: http://dx.doi.org/10.26583/bit.2022.1.07

Аннотация. Одним из наиболее перспективных решений оптимизации логистических процессов является создание автоматизированных систем управления поставками на основе технологии распределенного реестра, в частности смарт-контракта. Однако кроме известных экономических преимуществ такой технологии целесообразность ее практического применения будет во многом определяться устойчивостью функционирования указанных систем управления в современных условиях угрозы дестабилизирующих воздействий. В настоящее время решение вопросов безопасности смарт-контрактов, как прикладных программ, сводится к проверке исходного кода приложений. Очевидно, что этого явно недостаточно для обеспечения надежности логистического управления, устойчивость которого может быть определена на основе известных методов оценки комплексной безопасности соответствующей ИТ-системы. Целью данного исследования является адаптация существующих методов аудита и оценки рисков информационной безопасности для ИТ-системы, использующей смарт-контракт, а предметом – обоснование применимости такого подхода к оценке защищенности логистических процессов с учетом особенностей смарт-контрактов. В работе рассмотрены особенности применения смарт-контрактов в логистических процессах, изложены соответствующие подходы к аудиту и оценке рисков функционирования системы логистического управления на основе смарт-контрактов. Разработаны рекомендации по практической реализации конкретных методик оценки защищенности ИТ-системы, использующей смарт-контракт, что ставится авторами в качестве цели дальнейшей работы. Результаты исследования могут быть полезны специалистам в области оптимизации логистических процессов и обеспечения информационной безопасности при разработке новых логистических схем на основе смарт-контрактов.

Ключевые слова: аудит, информационная безопасность, ИТ-системы, логистические процессы, оценка защищенности, оценка рисков, распределенный реестр, смарт-контракт, устойчивость.
Для цитирования: ГОРБАТОВ, Виктор С.; ДЯТЛОВ, Дмитрий А.; НАТАЛИЧЕВ, Роман В. ОБ УСТОЙЧИВОСТИ ЛОГИСТИЧЕСКИХ СТРУКТУР НА ОСНОВЕ СМАРТ-КОНТРАКТОВ. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 70–81, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1403. DOI: http://dx.doi.org/10.26583/bit.2022.1.07.

Victor S. Gorbatov[1], Dmitriy A. Dyatlov[2], Roman V. Natalichev[3]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733
[2]e-mail: DADyatlov@mephi.ru, https://orcid.org/0000-0001-9967-6366
[3]e-mail: r.natalichev2015@yandex.ru, https://orcid.org/0000-0002-8985-7144

On the sustainability of logistics structures based on smart contracts

DOI: http://dx.doi.org/10.26583/bit.2022.1.07

Abstract. One of the most promising solutions for optimizing logistics processes is the creation of automated supply management systems based on distributed registry technology, in particular a smart contract. However, in addition to the well-known economic advantages of such a technology, the expediency of its practical application will largely be determined by the stability of the functioning of these

control systems in modern conditions of the threat of destabilizing influences. Currently, the solution to the security issues of smart contracts as programs are reduced to checking the source code of applications. Obviously, this is clearly not enough to ensure the reliability of logistics management, the stability of which can be determined on the basis of known methods for assessing the complex security of the corresponding IT system. This study adapts existing methods for auditing and assessing information security risks for an IT system using a smart contract, and the subject is to substantiate the applicability of such an approach to assessing the security of logistics processes, considering the features of smart contracts. The paper considers the features of the use of smart contracts in logistics processes, outlines appropriate approaches to audit and risk assessment of the functioning of the logistics management system based on smart contracts. Recommendations have been developed for the practical implementation of specific methods for assessing the security of an IT system using a smart contract, which is set by the authors as the goal of further work. The results of the study can be useful to specialists in the field of optimization of logistics processes and information security when developing new logistics schemes based on smart contracts.

Keywords: audit, information security, IT systems, logistics processes, security assessment, risk assessment, distributed ledger, smart contract, sustainability.

For citation: GORBATOV, Victor S.; DYATLOV, Dmitriy A.; NATALICHEV, Roman V. On the sustainability of logistics structures based on smart contracts. IT Security (Russia), [S.l.], v. 29, n. 1, p. 70–81, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1403. DOI: http://dx.doi.org/10.26583/bit.2022.1.07.

Введение

Развитие информационных технологий продолжает менять модель отношений не только в социальной, но и в профессиональной сферах, все больше переводя существующие процессы взаимодействия в виртуальную информационную среду. Наблюдается изменение средств и способов коммуникации, например, вследствие глобализации торговых отношений, что в свою очередь, ведет к изменению принципов взаимодействия между различными организациями, участвующими в логистических процессах. Появляется необходимость в квалифицированных сотрудниках логистических компаний вследствие применения новых технологических логистических решений, таких, например, как автоматизированные системы управления, электронная идентификация товаров и спутниковое слежение за движением транспортных потоков. Глобализация торговых отношений требует оптимизации существующих форм рыночных коммуникаций, что выражается в отчетливой тенденции к снижению издержек на логистические операции. В основном – это максимальное сокращение жизненного цикла процесса по перемещению готовой продукции или сырьевых товаров благодаря реорганизации цепей поставок, оптимизации транспорта, новых технологий, автоматизации складских работ и централизации доставки [1].

Однако множество причин препятствуют успешному преобразованию цепей поставок [2], характерных для большинства логистических структур:

– недостаточная проработка маршрутов поставок;

– простой на промежуточных узлах цепочек поставок;

– обеспечение безопасности, в том числе информационной, перемещения ценных грузов;

– несовершенство законодательной базы.

В последнее время снижение устойчивости логистических операций к воздействию дестабилизирующих факторов характеризуется таким кризисным явлением в мировой экономики как недостаток товаров даже в экономически развитых странах (США, Великобритании и др.), что явилось следствием произошедшей в 2020 г. пандемии коронавирусной инфекции, вскрывшей новые проблемы в мировой (глобальной) логистике [3]. В первую очередь – это отсутствие «антикризисного плана» в создавшейся обстановке всеобщей изоляции, и как следствие, снижение объема мировых логистических операций.

Основными дестабилизирующими факторами такого кризиса можно назвать недостаточно быструю переориентацию с одного вида транспортировки на другой, слабое внедрение и применение новейших информационных технологий, неготовность перевода сотрудников логистических компаний на удаленную работу с сохранением эффективности осуществляемых бизнес-процессов. Иными словами, основной фактор – неготовность существующей системы управления к новым вызовам.

В качестве конкретных примеров необходимости изменений в мире логистики можно привести аварию контейнеровоза «Эвер Гивен» с блокировкой Суэцкого канала и убытком для мировой логистики в 9,6 млрд долл./день [4], а также кибератаку на трубопроводную систему в США Colonial Pipeline в мае 2021 г. В результате кибератаки остановилась работа трубопровода [5], для возобновления функционирования которого компания заплатила злоумышленникам около 4,4 млн долл. В последнем случае сказалось недостаточно полное понимание проблем обеспечения информационной безопасности (ИБ) и, как следствие, низкая оперативность и реагирование на произошедший инцидент.

Тенденцией последних нескольких лет по совершенствованию управления и повышению устойчивости логистических структур стало все более широкое использование таких приложений как смарт-контракты, встроенные в распределенный реестр (РР) и систематизирующие эффективное взаимодействие между большим количеством пользователей при недостаточном или полном отсутствии доверия между ними [6]. Известными экономическими преимуществами смарт-контрактов являются более легкий и быстрый доступ к логистическим услугам и существующей инфраструктуре для обеспечения запасного транспортного канала [7], а также снижение количества сопроводительных документов, уменьшение дополнительных расходов для разрешения возникающих инцидентов, устранение операционных ошибок.

Постановка задачи и методология оценки рисков использования технологии РР как некоторой обобщенной ИТ-системы приведены в [8]. В настоящей работе эти вопросы рассмотрены применительно к такому приложению как смарт-контракт с учетом его особенностей.

1. Смарт-контракт как инструментарий повышения эффективности логистики

Идея смарт-контракта была предложена американским ученым Ником Сабо в 90-х годах прошлого века [9]. По сути, смарт-контракт – это компьютерная программа с заранее определенными протоколами, встраиваемая в оборудование или программное обеспечение для выполнения различных договорных условий. Система РР предоставляет среду коммуникаций, в которую можно поместить смарт-контракт для его непосредственной реализации.

Смарт-контракт автоматизирует проводимые транзакции по определенным правилам, например, действия могут выполняться строго при наступлении заданных событий, и выполнение данного алгоритма не может быть отменено, остановлено или заменено. В этом случае размещение в системе РР обеспечивает смарт-контракту взаимодействие с управляющей (выполнено условие или нет) и исполняющей (действие выполняется или нет) информацией. Жизненный цикл смарт-контракта[1] представлен на рис. 1.

[1]ISO/TR 23455:2019. Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems.

Рис. 1. Жизненный цикл смарт-контракта
Fig. 1. The life cycle of a smart contract

Прежде, чем создать контракт, необходимо договориться о его условиях: какие события ведут к каким действиям. Следующий шаг – создание самого смарт-контракта, то есть разработка алгоритма последовательности выполнения условий сделки и написание непосредственно программы. После этого смарт-контракт размещается в системе РР, чтобы все участники сделки видели и могли отслеживать прохождение этапов договора в рамках своих прав и компетенций. Затем смарт-контракт, как элемент системы РР, соединяется с внутренними и внешними источниками для получения и передачи данных для выполнения условий сделки. Когда все сформировано, смарт-контракт остается в положении ожидания внешнего события, прописанного в его алгоритме, и проверяет выполнение требований заключенной сделки. После наступления ожидаемого события происходит исполнение определенного действия смарт-контракта. До этого момента никаких действий в рамках смарт-контракта не происходит. Любые произошедшие изменения в системе записываются в реестр, реестр обновляется, и все участники системы видят, что происходит в реальном времени. Данные нельзя заменить, изменить, нельзя отказаться от совершенных действий, то есть обеспечиваются основные принципы ИБ – целостность и доступность используемых данных при обеспечении неотказуемости от совершенных действий. Еще один принцип ИБ – конфиденциальность соблюдается ввиду того, что каждый из участников системы обладает только информацией в рамках своих прав и своей компетенции. Остальная информация скрыта в «глубинах» смарт-контракта.

Для чего же все это надо? Сотни лет логистическая система работает по проверенным временем законам и принципам. Что дает данное новшество? Есть ли в этом какая-либо выгода или польза? Стоит ли усложнять «новомодными штучками» отработанный алгоритм действий. Рассмотрим это на примере поставки груза, рис. 2.

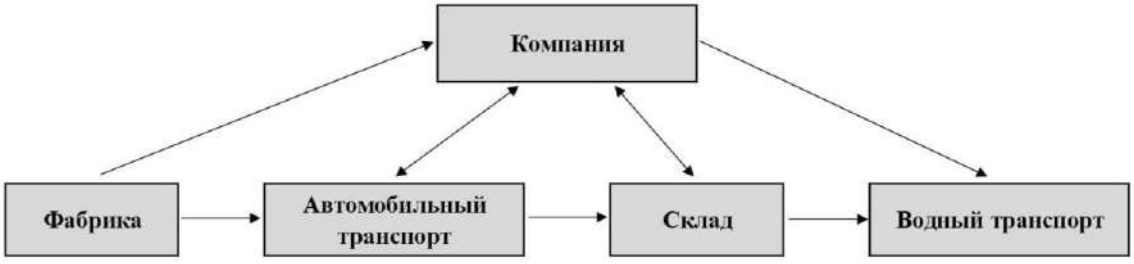


Рис. 2. Традиционная схема поставки груза
Fig. 2. Traditional cargo delivery scheme

Компания поставляет продукцию с фабрики двумя видами транспорта через промежуточный склад. При традиционной схеме поставки для прохождения этого процесса потребуется выполнение следующих операций:

1) отгрузка груза с фабрики на склад автомобильным транспортом;
2) сообщение с фабрики в компанию об отгрузке груза на склад;
3) сообщение из компании на склад об отгрузке в их адрес груза;
4) доставка груза на склад автомобильным транспортом;
5) сообщение со склада в компанию о доставке груза;
6) сообщение от автоперевозчика в компанию о доставке груза и счет за доставку;
7) оплата компанией доставки груза автоперевозчику;
8) заказ компании водного транспорта для отправки груза со склада;
9) отгрузка груза со склада для транспортировки водным транспортом;
10) сообщение со склада в компанию об отгрузке груза.

Такой же процесс по доставке груза с использованием смарт-контракта представлен на рис. 3.

Рис. 3. Схема поставки груза с использованием смарт-контракта
Fig. 3. Cargo delivery scheme using a smart contract

Для этой схемы поставки потребуется выполнение следующих информационных операций:

1) сообщение об отгрузке груза с фабрики записывается в смарт-контракт и автоматически передается в компанию и на склад;
2) сообщение о доставке груза на склад записывается в смарт-контракт и автоматически передается в компанию;
3) команда в компанию на оплату и оплата доставки груза автоперевозчику (выполняется смарт-контрактом автоматически);
4) заказ водного транспорта для отправки груза со склада (выполняется смарт-контрактом автоматически);
5) сообщение об отгрузке груза со склада записывается в смарт-контракт и автоматически передается в компанию.

Таким образом, при использовании смарт-контракта значительно сокращается количество ручных операций и время прохождения всех информационных процессов, в то время как в практике традиционных поставок для проведения подобных операций требуется время от нескольких часов до нескольких дней или даже недель. Нельзя забывать о том, что информационные процессы проходят через операторов, и чем больше участников

вовлечены в бизнес-операцию, тем большее количество людей в ней задействовано вместе с их оборудованием и сетями связи. Количество операторов при традиционной схеме гораздо больше, чем при использовании смарт-контракта. То есть снижается вероятность ошибок или утечки информации, а также возможность сговора отдельных участников между собой. Повышается «прозрачность» проводимой сделки и доверие между сторонами, участвующими в бизнес-операции.

Создание смарт-контракта исключает наличие иерархического управления, все участники контракта обладают равными правами, а операции выполняются по строго определенному алгоритму, то есть условия выполнения контракта не могут быть изменены в процессе его выполнения. Отсутствует возможность «давления» со стороны более сильного участника контракта на других участников, либо отказа от выполнения своих обязательств. Кроме этого, при несоблюдении условий контракта, штрафы и неустойки взыскиваются автоматически.

Размещение смарт-контракта в РР, то есть слияние двух самостоятельных технологий, создает систему смарт-контракта. Такая система отличается от первоначального замысла смарт-контракта [9] – набора обещаний, заданного в цифровой форме, для выполнения других обещаний, так как объединение с РР создает новое поколение независимых смарт-контрактов1. Такие системы имеют многоуровневую архитектуру [10], что требует соответствующих подходов и методов оценки их защищенности. В настоящее время нет общепринятой стандартной архитектуры РР с, размещенным в нем смарт-контрактом, поэтому в целях данной работы в основу исследования принята четырехуровневая модель архитектуры системы РР [8], представленная в табл. 1.

Таблица 1. Четырехуровневая модель архитектуры системы смарт-контракта

Уровень системы смарт-контракта	Уровень OSI	Технологические компоненты
Прикладной	Прикладной	Создание Интеграция Функционирование Приложения безопасности
Представления	Представления	Архитектура ПО, язык программирования Способы стимулирования Цифровые активы Функциональность Исполнение смарт-контрактов Управление правами доступа Способы увеличения пропускной способности
Транспортный	Сеансовый Транспортный	Консенсус Безопасность и приватность Исполнение транзакций
Физический	Сетевой Канальный Физический	Телекоммуникационные сети Телекоммуникационное оборудование Вычислительные системы

2. Постановка задачи исследования – оценка защищенности системы смарт-контракта

В настоящее время исследование смарт-контрактов проводится, в основном, на прикладном уровне и направлено на проверку исходного кода программ. Приложения

тестируются специалистами по ИБ, используя типовые подходы оценки надежности компьютерных программ, например, тестирование, проверка исходного кода и методология проектирования по контракту [11]. Но этих методов явно недостаточно при встраивании смарт-контрактов в систему РР, существующей и работающей в режиме реального времени, то есть при постоянном внесении изменений, в том числе в последовательность проводимых операций. И какой бы ни был объем тест-кейсов, он не в состоянии обеспечить достаточную проверку программного обеспечения. Следовательно, тестирование на прикладном уровне не может использоваться в качестве основного метода контроля защищенности системы смарт-контракта.

При функционировании смарт-контракта в РР блоки данных часто многократно обрабатываются различными узлами системы, то есть к уровню приложений относятся не только смарт-контракты. Также на этом уровне находятся программы, обеспечивающие взаимодействие между узлами РР, влияющие на:

- работу смарт-контракта,
- обмен данными и цифровыми активами,
- программы наблюдения за загрузкой данных и состоянием системы,
- программы отслеживания проводимых операций,
- программы защиты сети, резервного копирования и восстановления системы.

В этих программах и на других уровнях архитектуры системы также могут возникнуть уязвимости.

Таким образом, известные в настоящее время методы, применяемые для обеспечения ИБ смарт-контрактов, не учитывают в полной мере особенности архитектуры встраивания этих приложений в системы и сети бизнес-процессов. Требуется более детальный и всеобъемлющий подход к обеспечению безопасности таких систем, позволяющий определить потребности в защите информации и создании эффективной системы управления. Необходимо обеспечить своевременное реагирование на возникающие инциденты ИБ и применение технических, организационных, программных, правовых и других защитных мер для минимизации вероятности возникновения инцидентов.

Практическая реализация смарт-контрактов и перспективы их дальнейшего развития зависят от соблюдения основных принципов обеспечения ИБ, таких как аутентификация и обеспечение неотказуемости для участников сети, обеспечение надежности системы криптографическими ключами. Данные принципы либо игнорируются, либо им придается недостаточное значение, что приводит к отсутствию доверия и признанию их пока ненадежными системами, подверженными колоссальному риску [12].

Еще одним «слабым» звеном ИБ системы РР с размещенным в нем смарт-контрактом является обеспечение конфиденциальности, в частности данных проводимых транзакций, которые записываются в реестр. В этом направлении ведутся активные научные и практические работы, изучающие различные инструменты обеспечения конфиденциальности проводимых операций в системах РР, например: «Криптографические перемешивающие сети», «Кольцевая подпись», «Гомоморфное шифрование», «Доказательства с нулевым разглашением» [13]. Но, на данный момент, ни один из существующих методов не решает удовлетворительно эту проблему в целом, относительно производительности и объема данных, которые создаются участниками сети в процессе проведения транзакций [13].

Для решения проблем унификации технологии РР в 2016 г. был образован специализированный технический комитет ISO/TC 307 «Технологии блокчейна и распределенного реестра». Этот комитет ведет работу над десятью стандартами данных

технологий [14]. На сегодняшний день только четыре стандарта опубликованы, причем три из них в 2020 г. Первый стандарт ISO 23455 «Обзор и взаимодействие между смарт-контрактами в системах технологии блокчейна и технологий распределенного реестра» был опубликован в сентябре 2019 г., на основании которого и проходит проверка ИБ в отношении смарт-контрактов.

Для успешного интегрирования смарт-контракта, представляющего в совокупности с технологией PP ИТ-систему, в логистические процессы необходимо реализовать комплексный подход к обеспечению ИБ, определяющей устойчивость логистики на протяжении всего жизненного цикла существования системы – от планирования до эксплуатации и сопровождения. Иными словами, необходима организация систематического процесса, оценивающего все составляющие логистической системы, обеспечивающий безопасность проводимых операций и осуществляющий управление ИБ.

3. Методология оценки защищенности системы смарт-контракта

Наиболее полно решению поставленной выше задачи отвечает известная методология [15], предусматривающая совокупность организационных процедур, условно разделенных на три этапа:

- подготовительный,
- основной,
- заключительный.

Практическую реализацию указанных процедур можно проводить в рамках аудита ИБ, который наиболее полно отвечает требованиям по оценке защищенности информационных систем управления. По результатам аудита ИБ осуществляется принятие и выполнение решений по ИБ на всех этапах жизненного цикла, выявляются возможные уязвимости, повышается эффективность использования имеющихся технологических ресурсов.

Важнейшим элементом аудита, часто выделяемым в отдельную задачу, является совокупность процедур оценки рисков. Такая оценка позволяет определить ценность используемых данных и других активов системы, связанные с ними уязвимости и угрозы устойчивости системы, расставить их в приоритетном порядке с целью более эффективного распределения технологических ресурсов. Методология оценки рисков ИБ ИТ-систем в настоящее время хорошо изучена, достаточно унифицирована, имеет обширный опыт применения [16], что позволяет рассматривать ее в качестве основы для дальнейшей адаптации в целях оценки защищенности системы смарт-контракта.

Обобщенный процесс проведения оценки рисков и дальнейших мероприятий по их управлению применительно к системе смарт-контракта, в соответствии с [16–17], представлен на рис. 4.

Рис. 4. Оценка рисков ИБ системы смарт-контракта
Fig. 4. Risk assessment of the information security of the smart contract system

В зависимости от принятых в конкретной логистической структуре управленческих взаимодействий процедуры оценки рисков могут значительно различаться по методам, требованиям и масштабу, но основной их целью остается выявление рисков для активов структуры, а также их количественная и качественная оценки. Количественный и качественный метод – два основных подхода к оценке рисков ИБ [17], применяемые независимо друг от друга или одновременно, наиболее полно представлены в стандарте, использованном в [8] для системы РР. По аналогии для системы смарт-контракта можно рекомендовать к использованию те же методы оценки рисков:

1) «Анализ дерева отказов (FTA)»,
2) «Анализ надежности человека (HRA)»,
3) «Изучение опасности и работоспособности (HAZOP)»,
4) «Методы нечеткой логики»,
5) «Техническое обслуживание на основе надежности (RCM)».

В [8] также предложена алгоритмическая основа, которую можно использовать для практической реализации типовой методики оценки рисков системы смарт-контракта на базе «хорошей практики», предлагающей известный итеративный подход к проведению оценки рисков. Итоговый алгоритм применительно к системе смарт-контракта представлен на рис. 5.

Рис. 5. Алгоритм оценки рисков ИБ системы смарт-контракта
Fig. 5. Algorithm for assessing the risks of information security of the smart contract system

Приведенные выше методы не покрывают полностью процесс проведения оценки рисков ИБ и рекомендуются только как основа для адаптации существующих и создания новых технологий оценки рисков системы смарт-контракта. Необходимы комплексные мероприятия, сочетающие применение нескольких методов и технологий оценки рисков ИБ одновременно на соответствующих этапах проведения проверки. То есть разработка конкретной методики не должна строго ограничиваться методами, определенными в данной работе, и в дальнейшем допускается совместное использование с другими технологиями.

Также важным элементом методики является этап документирования всех результатов оценки защищенности системы смарт-контракта, на основе которого создается политика безопасности системы и составляется план управления рисками ИБ.

Заключение

Существующая тенденция по совершенствованию управления и повышению устойчивости логистических структур актуализирует все более широкое использование таких приложений, как смарт-контракты, встроенные в систему распределенного реестра. Смарт-контракты систематизируют эффективное взаимодействие между пользователями при недостаточном или полном отсутствии доверия между ними.

В то же время, их практическое внедрение во многом сдерживается из-за нерешенности многих вопросов обеспечения ИБ не столько на прикладном, сколько на системном уровне. Представленные в работе подходы по решению поставленной задачи создают методологическую основу для дальнейшего развития исследований в направлении разработки типовых методик оценки защищенности системы смарт-контракта с использованием хорошо зарекомендовавших себя методов аудита и управления рисками ИБ.

СПИСОК ЛИТЕРАТУРЫ:

1. Белякова А.В. Значение логистики в условиях глобализации международного товародвижения. E-SCIO. 2020, № 4 (43), с. 597–607. URL: https://elibrary.ru/item.asp?id=42818426 (дата обращения 17.01.2022).
2. Захарова А.И. Основные проблемы транспортной логистики в России. Аллея науки. 2020, т. 2, № 4 (43), с. 7–10. URL: https://elibrary.ru/item.asp?id=42951263 (дата обращения 17.01.2022).
3. Воронецкий Д.А. Логистические тренды 2020–2021 года: жизнь во время и после пандемии. The scientific heritage. 2021, № 75–4 (75), с. 23–29. DOI: https://doi.org/10.24412/9215-0365-2021-75-4-23-29.
4. Калинина А.А. Особенности морских перевозок на примере Суэцкого канала. Известия института систем управления СГЭУ. 2021, № 1 (23), с. 123–125. URL: https://www.elibrary.ru/item.asp?id=45849004 (дата обращения 17.01.2022).
5. Демидов А. Глава Colonial Pipeline рассказал, сколько компания заплатила хакерам. Газета.ru. 19.05.2021. URL: https://www.gazeta.ru/tech/news/2021/05/19/n_15997772.shtml (дата обращения 17.01.2022).
6. Дмитриев А.В. Развитие технологии блокчейн в транспортно-логистических системах. Логистика – евразийский мост. Материалы XIV Международной научно-практической конференции. Красноярск, 24–29 апреля 2019. С. 98–103. URL: https://www.elibrary.ru/item.asp?id=37383916 (дата обращения 17.01.2022).
7. Irannezhad E. Is blockchain a solution for logistics and freight transportation problems? Transportation Research Procedia. 2020, vol. 48, p. 290–306. DOI: https://doi.org/10.1016/j.trpro.2020.08.023.
8. Durakovskiy A.P., Gorbatov V.S., Melnikov D.A., Dyatlov D.A. Security risk management methodology for distributed ledger systems. Conference: BICA*AI 2021: BICA Workshop at ACM IVA 2021, a virtual event. Fukuchiyama, Kyoto, Japan, September 14, 2021. SCI 1032, p. 1–17. DOI: https://doi.org/10.1007/978-3-030-96993-6_9.
9. Nick Szabo. Smart Contracts: Building Blocks for Digital Markets. 1996. URL:https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (дата обращения 17.01.2022).
10. Запечников Сергей В. Системы распределенного реестра как инструмент обеспечения доверия между участниками бизнес-процессов. Безопасность информационных технологий, [S.l.], т. 26, № 4, с. 37–53. 2019. DOI: http://dx.doi.org/10.26583/bit.2019.4.03.
11. Меркин Л.А., Резин Р.М., Васильев Н.К. Архитектура формально-верифицированной системы распределенного реестра InnoChain. Моделирование и анализ информационных систем. 2020, т. 27, № 4, с. 472–487. DOI: https://doi.org/10.18255/1818-1015-2020-4-472-487.
12. Будзко Владимир И., Мельников Дмитрий А. Исторический ракурс технологии «Blockchain». «Всё новое – хорошо забытое старое». Безопасность информационных технологий, [S.l.], т. 25, № 4, с. 23–33, 2018. DOI: http://dx.doi.org/10.26583/bit.2018.4.02.
13. Запечников Сергей В. Системы распределенного реестра, обеспечивающие конфиденциальность транзакций. Безопасность информационных технологий, [S.l.], т. 27, № 4, с. 108–123, 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.09.
14. Будзко Владимир И., Милославская Наталья Г. Вопросы практического применения технологий блокчейна. Безопасность информационных технологий, [S.l.], т. 26, № 1, с. 36–45, 2019. DOI: http://dx.doi.org/10.26583/bit.2019.1.04.
15. Макаренко С. И. Аудит ИБ: основные этапы, концептуальные основы, классификация мероприятий. Системы управления, связи и безопасности. 2018, № 1, с. 1–29. URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf (дата обращения 17.01.2022).
16. Кривякин К.С., Изотова А. Р., Федоров В. М. Методический подход к оценке рисков информационной безопасности предприятия. Экономинфо. 2018, т. 15, № 2, с. 82–90. URL: https://elibrary.ru/item.asp?id=35177684 (дата обращения 17.01.2022).
17. Склярук В.Л., Сергеева О.О. Методы оценки рисков информационной безопасности. Современные проблемы радиоэлектроники и телекоммуникаций. 2018, № 1, с. 219. URL: https://elibrary.ru/item.asp?id=38500295 (дата обращения 17.01.2022).

REFERENCES:

[1] Belyakova A.V. The significance of logistics in the context of globalization of international commodity circulation. E-SCIO. 2020, no. 4 (43), p. 597–607. URL: https://elibrary.ru/item.asp?id=42818426 (accessed: 17.01.2022) (in Russian).
[2] Zakharova A.I. The main problems of transport logistics in Russia. Alley science. 2020, vol. 2, no. 4 (43), p. 7–10. URL: https://elibrary.ru/item.asp?id=42951263 (accessed: 17.01.2022) (in Russian).
[3] Voronetskiy D.A. Logistics trends of 2020-2021: life during and after the pandemic. The scientific heritage. 2021, no. 75–4 (75), p. 23–29. DOI: https://doi.org/10.24412/9215-0365-2021-75-4-23-29 (in Russian).

[4] Kalinina A.A. Features of shipping on the example of the suez canal. News of the Institute of Control Systems SSUE. 2021, no. 1 (23), p. 123–125. URL: https://www.elibrary.ru/item.asp?id=45849004 (accessed: 17.01.2022) (in Russian).
[5] Demidov A. The head of Colonial Pipeline told how much the company paid hackers. Gazeta.ru. 19.05.2021. URL: https://www.gazeta.ru/tech/news/2021/05/19/n_15997772.shtml (accessed: 17.01.2022) (in Russian).
[6] Dmitriev A.V. Development of blockchain technology in transport and logistics systems. Logistics – Eurasian bridge. Materials of the XIV International Scientific and Practical Conference. Krasnoyarsk, 24–29 April 2019. P. 98–103. URL: https://www.elibrary.ru/item.asp?id=37383916 (accessed: 17.01.2022) (in Russian).
[7] Irannezhad E. Is blockchain a solution for logistics and freight transportation problems? Transportation Research Procedia. 2020, vol. 48, p. 290–306. DOI: https://doi.org/10.1016/j.trpro.2020.08.023.
[8] Durakovskiy A.P., Gorbatov V. S., Melnikov D.A., Dyatlov D.A. Security risk management methodology for distributed ledger systems. Conference: BICA*AI 2021: BICA Workshop at ACM IVA 2021, a virtual event. Fukuchiyama, Kyoto, Japan, September 14, 2021. SCI 1032, p. 1–17. DOI: https://doi.org/10.1007/978-3-030-96993-6_9.
[9] Nick Szabo. Smart Contracts: Building Blocks for Digital Markets. 1996. URL:https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (accessed: 17.01.2022)
[10] Zapechnikov Sergey V. Distributed ledger as a tool to ensure trust among business process participants. IT Security, [S.l.], vol. 26, no. 4, p. 37–53, 2019. DOI: http://dx.doi.org/10.26583/bit.2019.4.03 (in Russian).
[11] Merkin-Janson L.A., Rezin R.M., Vasilyev N.K. Architecture of the Formally-Verified Distributed Ledger System InnoChain. Modeling and Analysis of Information Systems. 2020, vol. 27, no. 4, 472–487. DOI: https://doi.org/10.18255/1818-1015-2020-4-472-487.
[12] Budzko Vladimir I., Melnikov Dmitry A. The historical view of the blockchain technology. The more things change, the more they stay the same. IT Security, [S.l.], vol. 25, no. 4, p. 23–33, 2018. DOI: http://dx.doi.org/10.26583/bit.2018.4.02 (in Russian).
[13] Zapechnikov Sergey V. The distributed ledgers ensuring privacy-preserving transactions. IT Security, [S.l.], vol. 27, no. 4, p. 108–123, 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.09 (in Russian).
[14] Budzko Vladimir I., Miloslavskaya Natalia G. Issues of practical application of blockchain technology. IT Security, [S.l.], vol. 26, no. 1, p. 36–45, 2019. DOI: http://dx.doi.org/10.26583/bit.2019.1.04 (in Russian).
[15] Makarenko S.I. Audit of information security - the main stages, conceptual framework, classification of types. Systems of control, communication and security. 2018, no. 1, p. 1–29. URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf (accessed: 17.01.2022) (in Russian).
[16] Krivyakin K.S., Izotova A.R., Fedorov V.M. Methodological approach to risk assessment the enterprise information security. Economінfo. 2018, vol. 15, no. 2, p. 82–90. URL: https://elibrary.ru/item.asp?id=35177684 (accessed: 17.01.2022) (in Russian).
[17] Sergeeva O.O., Sklyaruk V.L. Methods of estimation of information security risk. Modern problems of radio electronics and telecommunications. 2018, no. 1, p. 219. URL: https://elibrary.ru/item.asp?id=38500295 (accessed: 17.01.2022) (in Russian).

Поступила в редакцию – 21 января 2022 г. Окончательный вариант – 15 февраля 2022 г.
Received – January 21, 2022. The final version – February 15, 2022.

Сергей В. Дуга[1], Виктория В. Ефимова[2], Андрей И. Труфанов[3]
[1]Судебно-экспертный центр Следственного комитета Российской Федерации,
Строителей ул., 8, корпус 2, Москва, 119313, Россия
[2]Следственное управление Следственного комитета Российской Федерации
по Иркутской области,
Володарского ул., 11, Иркутск, 664011, Россия
[3]Иркутский национальный исследовательский технический университет,
Лермонтова ул., 83, Иркутск, 664074, Россия
[1]e-mail: siber@list.ru, https://orcid.org/0000-0002-5894-9855
[2]e-mail: efimova.vika1977@mail.ru, https://orcid.org/0000-0003-3990-1917
[3]e-mail: troufan@gmail.com, https://orcid.org/0000-0002-6967-3495

АЛГОРИТМЫ СЕТЕВОГО АНАЛИЗА ДАННЫХ В РАСКРЫТИИ СХЕМЫ НАЛОГОВОГО ПРЕСТУПЛЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2022.1.08

Аннотация. В статье рассматривается возможность применения средств сетевого (графового) анализа при раскрытии схемы налогового преступления и формировании стратегии его расследования. Предложена модель данных, позволяющая построить сетевую топологию преступления основываясь как на непосредственных материалах о событии преступления, так и на дополнительной информации, полученной путем доступа к базам данных правоохранительных и контрольных органов. Рассмотрены алгоритмы сетевого анализа, способствующие выявлению новых сведений о преступной схеме. Данные сетевые алгоритмы позволяют обнаружить скрытые и неочевидные связи между фигурантами дела, выявить иерархическую структуру их отношений, что способствует установлению ключевых участников преступной схемы. На примерах различных уголовных дел налоговых преступлений показано, что применение сетевого анализа данных позволяет сформировать схему преступления, дать правильную криминалистическую характеристику преступления, определить круг его субъектов, предложить следователю криминалистическую методику расследования данного вида преступлений (алгоритм расследования) и типовые следственные версии, что в совокупности способствует организации расследования должным образом.

Ключевые слова: сетевой анализ, налоговые преступления, схема налогового преступления, алгоритмы сетевого анализа, расследование преступлений.

Для цитирования: ДУГА, Сергей В.; ЕФИМОВА, Виктория В.; ТРУФАНОВ, Андрей И. АЛГОРИТМЫ СЕТЕВОГО АНАЛИЗА ДАННЫХ В РАСКРЫТИИ СХЕМЫ НАЛОГОВОГО ПРЕСТУПЛЕНИЯ. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 82–93, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1409. DOI: http://dx.doi.org/10.26583/bit.2022.1.08.

Sergey V. Duga[1], Viktoriya V. Efimova[2], Andrey I. Trufanov[3]
[1]Forensic Expert Center of the Investigative Committee of the Russian Federation,
Stroitelej str., 8, k. 2, Moscow, 119313, Russia
[2]Investigative Committee of the Russian Federation Irkutsk Region,
Volodarskogo str., 11, Irkutsk, 664011, Russia
[3]Irkutsk National Research Technical University,
Lermontova str., 83, Irkutsk, 664074, Russia
[1]e-mail: siber@list.ru, https://orcid.org/0000-0002-5894-9855
[2]e-mail: efimova.vika1977@mail.ru, https://orcid.org/0000-0003-3990-1917
[3]e-mail: troufan@gmail.com, https://orcid.org/0000-0002-6967-3495

Algorithms of network data analysis in the disclosure of a tax crime scheme

DOI: http://dx.doi.org/10.26583/bit.2022.1.08

Abstract. The paper considers the possibility of using network (graph) analysis tools in the disclosure of a tax crime scheme and the formation of a strategy for its investigation. A data model is proposed that allows building a network topology of a crime based both on direct material about a crime event and on additional information obtained by accessing the databases of law enforcement and control agencies. The algorithms of network analysis that contribute to the identification of new information about the criminal scheme are also considered. These network algorithms make it possible to detect hidden and non-obvious connections between the defendants in the case, to identify the hierarchical structure of their relationships, which helps to identify the key participants in the criminal scheme. Using the examples of various criminal cases of tax crimes, it is shown that the use of the considered variants of network data analysis allows forming a crime scheme, providing the correct criminalistic characterization of the crime, determining the range of its subjects, offering the investigator a forensic methodology for investigating this type of crime (investigation algorithm) and standard investigative versions, that all together contribute to the proper organization of the investigation.

Keywords: mathematical modeling network analysis, tax crimes, tax crime scheme, network analysis algorithms, crime investigation.

For citation: DUGA, Sergey V.; EFIMOVA, Viktoriya V.; TRUFANOV, Andrey I. Algorithms of network data analysis in the disclosure of a tax crime scheme. IT Security (Russia), [S.l.], v. 29, n. 1, p. 82–93, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1409. DOI: http://dx.doi.org/10.26583/bit.2022.1.08.

Введение

Расследование преступления – сложный интеллектуальный процесс, в котором задействованы множество механизмов. Специалист в процессе расследования сталкивается со значительным числом трудностей, главный из которых – ограниченность временных ресурсов для установления всех обстоятельств преступления и завершения расследования. У каждого вида преступлений своя специфика и особенности при выборе стратегии и тактики расследования. Вместе с тем выделяется категория «интеллектуальных» преступлений, раскрытие которых напрямую зависит от правильности сбора первичного аналитического материала и способностей его анализа. В их числе налоговые преступления.

Предложенные в научной и практической литературе алгоритмы расследования налоговых преступлений не могут претендовать на всеохватность. Каждое преступление индивидуально, а применяемые криминальные схемы уникальны. Поэтому на первый план выходит способность подхода к сбору и анализу информации, формированию схемы преступления. От правильно построенной схемы налогового преступления зависит оперативность в расследовании и возможность применения превентивных мер к их совершению, обеспечение возмещения ущерба, причиненного государству.

В настоящее время на практике следователь является единственным лицом, который фиксирует ход следствия в установленном законом порядке, проводит аналитику собранных доказательств и обеспечивает выявление новых составов преступлений. Многие правоохранительные и контрольные органы имеют специализированные подразделения, включающие группы лиц, занимающихся отдельными направлениями процесса по выявлению фактов уклонения от уплаты налогов, и осуществляющих аналитику. Следователь такой поддержки лишен, так как в структуре Следственного комитета РФ отсутствуют собственные оперативные подразделения, а также аналитические службы, которые могли бы облегчить следователю процесс выявления преступления и формирования доказательств. При этом сбор информации для анализа, позволяющий отнести его результаты к доказательствам, осуществляется следователем в отсутствие каких-либо специфических программных комплексов, в так называемом «ручном» режиме, что существенно растягивает во времени процесс расследования.

Доказывание начинается со сбора информации для формирования схемы преступления. На данном этапе важнейшее значение приобретает оперативность получения

значимой информации из различных источников, формирование собственной базы данных, содержащей сведения об участии потенциальных субъектов схемы в преступной деятельности, связь таких субъектов с иными субъектами в схеме.

Традиционно, налоговые преступления отличаются длительностью их совершения, системным характером преступных действий и их проработанностью. Сбор аналитического материала для выявления и расследования налогового преступления осуществляется из огромного числа источников, наиболее значимые из них – базы данных налоговых, регистрирующих органов, коммерческих банков, таможенных органов, судов. Получение информации из таких источников в настоящее время занимает значительное время, осуществляется в формате «запрос-ответ» в бумажном виде, имеет ограниченный формат. Впоследствии полученные сведения следователь аккумулирует и обобщает, составляя схему преступления.

Применение средств сетевого анализа при раскрытии схемы налогового преступления и формировании стратегии и тактики расследования способно существенно облегчить процесс доказывания, оптимизировать работу следователя и сократить сроки расследования уголовных дел.

1. Обзор работ, близких по тематике

В настоящее время, со стороны исследователей всего мира, наблюдается рост интереса к применению новейших методов анализа данных для борьбы с преступностью в общем контексте [1–4], так и для расследования налоговых преступлений [5–7].

В [8] предложена аналитическая система для выявления влиятельных членов преступной организации. Подход состоит из последовательных этапов:

1) построение сети (сеть создается либо из данных мобильной связи, поддерживаемой преступной организацией, либо из отчетов о преступлениях, содержащих информацию о членах преступной организации),

2) назначение веса каждой связи в сети (вес связи представляет собой количество телефонных звонков/сообщений между двумя преступниками),

3) вычисление кратчайшего пути по степени посредничества (мера, которая отражает значимость узла (вершины) при передаче информации из одной части сети в другую),

4) присвоение оценки каждому узлу в сети на основе концепции зависимости существования. Преступники, представленные узлами (вершинами) высшего ранга, считаются влиятельными членами преступной организации.

В [9] представлена аналитическая система «ATTENet», предназначенная для обнаружения и объяснения подозрительных групп уклонения от уплаты налогов на основе аффилированных транзакций. Для решения задачи, во-первых, система создает сеть, которая включает данные о налогах и налогоплательщиках из официальной налоговой базы данных. Затем система объединяет основные характеристики и особенности структуры каждой группы в сети методом «Structure2Vec», после чего, с использованием алгоритма «Random Forest», обнаруживает подозрительные группы. Наконец, для изучения и объяснения результатов, система предоставляет визуализацию с интерактивными инструментами.

2. Используемые источники данных

Для наполнения информационной системы сведениями, нами используются различные источники. Кратко перечислим их:

– материалы уголовных дел. На текущий момент используется система «Pullenti» [10] для извлечения именованных сущностей и семантического анализа материалов уголовных дел, в частности протоколов допросов. На рис. 1 представлен пример такого анализа. Из первоначального текста извлекаются именованные сущности, а также, в результате семантического анализа, строится сетевая модель;

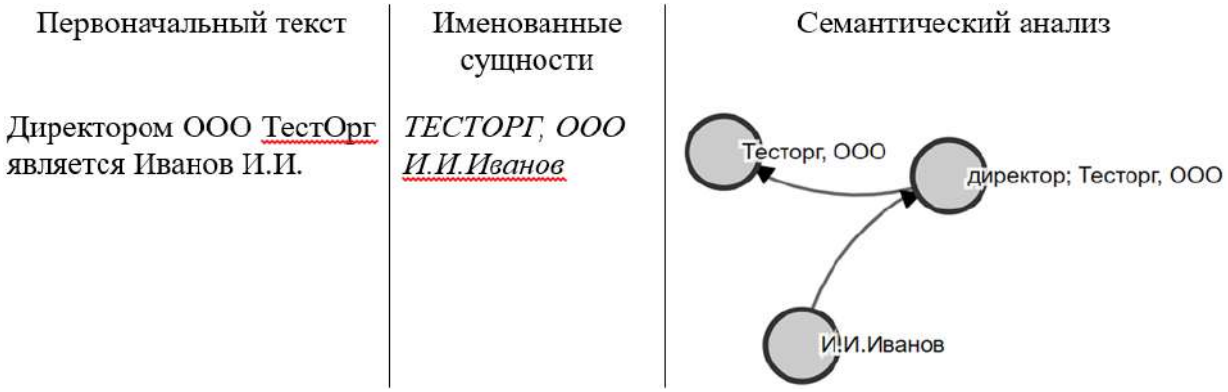


Рис. 1. Пример анализа текста с использованием системы «Pullenti»
Fig. 1. An example of text analysis using the "Pullenti" system

– данные из мобильных телефонов. По результатам осмотров мобильных телефонов фигурантов уголовных дел формируются отчеты, которые, в последующем, загружаются в систему. Использование средств коммуникации, таких как телефонные звонки и мессенджеры, оставляют цифровые следы, которые можно использовать для анализа. Это позволяет следователям лучше понимать внутреннюю иерархию преступных организаций, обнаруживая субъектов, которые играют центральную роль и/или обеспечивают связь между подгруппами;

– сведения от налоговых органов.

Также в систему загружаются сведения из программ учета финансово-хозяйственной деятельности, полученные в ходе производства осмотров электронных носителей информации, данные из единой информационной системы в сфере закупок, результаты арбитражных процессов.

3. Модель данных

Налоговое преступление, как правило, представляет собой сложную систему – совокупность объектов и субъектов, взаимодействующих друг с другом нетривиальным образом. При расследовании данного вида преступлений важно проводить анализ сети в целом, не сосредоточивая внимание на отдельных субъектах. Такой тип оценки может существенно выиграть от применения сетевого анализа, когда лица рассматриваются как акторы, которые связаны друг с другом в рамках взаимозависимой системы.

Чтобы изучить сложные системы в разных дисциплинах и областях, первым шагом является конкретное представление системы с использованием унифицированного математического языка. Кроме того, эти формализмы позволяют конструировать эффективные алгоритмы и могут использоваться для определения структуры, функции и динамики системы. Представляя исследуемые структуры в виде сетей, можно применять различные математические и сетевые методы для количественной оценки и выявления структурных особенностей.

В данном исследовании используется сетевая модель, которую можно представить в виде кортежа (*V, E, L(V), T(E), X*), представляющая собой неориентированный граф, вершины и ребра которого связаны с одной или несколькими метками, где:

V – множество вершин,

E – множество ребер,

L(V) – сюръективное отображение (v , l), которое связывает вершины с метками, такое, что каждой вершине $v \in V$, соответствует хотя бы одна метка $l \in L$,

T(E) – сюръективное отображение (e , t), которое связывает ребра с их типами, такое, что каждому ребру $e \in E$ соответствует хотя бы один тип $t \in T$.

Кроме того, каждая вершина связана с соответствующим вектором признаков. Здесь *X* является матрицей признаков для графа ($X \in \Re^{N \times D}$), так, что *i*-я строка *X* является вектором признаков для узла $v_i (i = 1,2 \ldots .|V|)$.

Для дальнейшего численного анализа определим матрицу смежности ($A^{N \times N}$) данного графа, такую что:

$$A_{ij} \begin{cases} 1, \text{если существует связь между вершинами } i \text{ и } j \\ 0, \quad \text{в ином случае} \end{cases}.$$

Кроме того, используются двудольные сети для разделения неоднородного графа на однородные подграфы, с целью последующего анализа. В двудольных графах вершины разбиты на два непересекающихся подмножества, так, что связи (ребра) могут возникать только в том случае, если вершины принадлежат разным множествам. Применение двудольных сетей (графов) может использоваться для представления связей субъект-организация, когда один тип представляет исходные узлы (например, люди), а другой представляет группы, к которым принадлежит первый тип узлов (например, организация). Двудольная сеть и ее граф определяется матрицей инцидентности ($A^{N \times G}$). Например, если имеется *n* субъектов и *g* организаций:

$$A_{ij} \begin{cases} 1, \text{если } j \text{ субъект принадлежит к организации } i \\ 0, \text{ в ином случае} \end{cases}.$$

Основываясь на предложенных в [11, 12] моделях, узлы используются для представления, таких сущностей как:

– Субъекты. Физические лица, имеющие отношение к расследуемому уголовному делу.

– Организации. Юридические лица, имеющие отношение к расследуемому уголовному делу.

– События – время, место, способ и другие обстоятельства совершения преступления, обстоятельства, способствовавшие совершению преступления (УПК РФ статья 73), а также иные обстоятельства, имеющие значение для уголовного дела (встречи людей, телефонные звонки, передача данных и пр.).

– Объектами могут быть любые предметы, которые служили орудиями, оборудованием или иными средствами совершения преступления, предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела (УПК РФ статья 81).

– Места – место совершения преступления, домашний/рабочий адрес человека, адрес регистрации юридического лица и пр.

В зависимости от типов узлов используются различные связи между ними, например, связь между организацией и физическим лицом, а также между организациями, может быть установлена из программ учета финансово-хозяйственной деятельности

организаций, сведений, полученных из налогового органа или вручную. В свою очередь, связь между физическими лицами может быть охарактеризована различными типами: родственники, коллеги, частое общение, общаются редко. Тип связи задается вручную, или определяется автоматически на основе анализа телефонных соединений, обмена сообщениями и иных источников. Для иллюстрации изложенного на рис. 2 приведена часть концептуальной модели данных, сформированной в графовой базе данных «Neo4j».

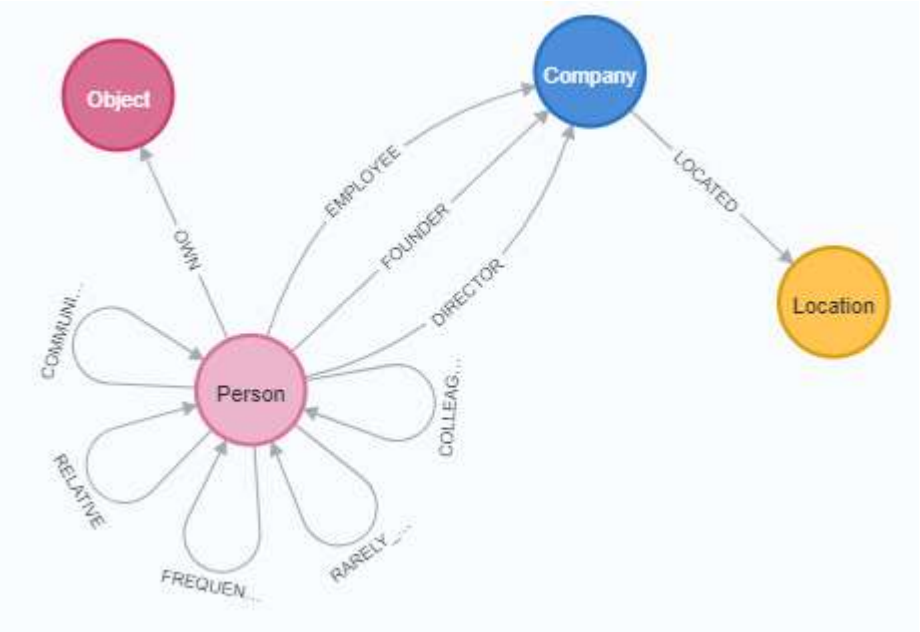


Рис. 2. Часть концептуальной модели данных
Fig. 2. Part of the conceptual data model

Сеть строится на основе данных, получаемых в рамках расследования уголовного дела, предполагая, как ручное внесение данных, так и автоматическое извлечение сведений из различных источников.

4. Используемые алгоритмы сетевого анализа

Анализ отношений между физическими и юридическими лицами представляет собой выявление и определение степени (важности) личных связей, имущественных прав. Такие связи могут быть как формальными, так и неформальными. Формальные связи легко проверить с помощью соответствующих документов и реестров. Неформальными связи можно определить на основе различных данных, полученных в ходе расследования преступления, например сведения о телефонных соединениях или финансовые операции. Анализ, основанный на различных источниках данных, также позволяет определить роль отдельных узлов во всей сети.

В ходе анализа связей необходимо, в частности, выявить следующие признаки аффилированности:

– участие одних и тех же лиц в создании, управлении организациями, в том числе через родственников или подконтрольных лиц;

– пересечение по работе в одной и той же организации, т.е. либо одновременно являются работниками организации, либо работали в ней в разное время;

– совпадение адресов государственной регистрации организаций.

5. Прогноз существования связи

Данную задачу можно сформулировать следующим образом:

Если имеется набор данных в виде сети $G = (V, E)$, где V – множество узлов, E – множество наблюдаемых связей, то задача заключается в том, чтобы предсказать, насколько вероятно существование ненаблюдаемой связи ($e_{ij} \notin E$) между произвольной парой узлов v_i, v_j.

Для решения подобных задач используются различные методы [13–15]. Одним из таких методов является метод «Общие соседи» (Common Neighbors) [16]. В основе данного метода лежит предположение, что два узла с большой вероятностью связаны между собой (они будут связаны в ближайшем будущем), если у них много общих соседей:

$$score(x, y) = |\Gamma(x) \cap \Gamma(y)|,$$

где $\Gamma(x)$ –набор узлов, смежных с узлом x, а $\Gamma(y)$ –набор узлов, смежных с узлом y.

Применение данного метода целесообразно ввиду того, что, зачастую, у следователя есть только частичная информация для анализа.

Несмотря на свою простоту, метод хорошо работает в большинстве реальных сетей и превосходит сложные подходы [17]. Например, при расследовании уголовного дела по факту хищения бюджетных средств путем незаконного возмещения НДС с деятельности ООО Б. в особо крупном размере решение о потенциальному круге фигурантов уголовного дела (Р., Ф., С.) сделан следователем с учетом данных о связях лица Р., заявленного в уставных документах в качестве руководителя организации, с иными лицами, хотя и не имеющими официального отношения к Обществу, но фактически являющимися его руководителями.

В ходе расследования были получены сведения от налогового органа о лицах, заявленных в качестве работников ООО Б., сведения из базы ЕГРЮ, сведения от кредитных организаций по месту открытия расчетных счетов общества. На основании полученных сведений была построена сетевая модель преступления и применен метод прогноза существования связи, который показал высокую вероятность наличия связи между ООО Б. и физическими лицами Ф. и С.

6. Использование метрики «центральность по собственному вектору»

Целью данной метрики является определение наиболее значимых фигурантов уголовного дела путем присваивания веса каждой вершине в сети посредствам использования алгоритмов центральности [18–21].

На основе предложенной модели вычисляются степени значимости (определение важности отдельных узлов в сети) как классическими методами сетевого анализа, так и методами, адаптированными для предметной области (предварительное следствие). Основная цель этой оценки – выявить те субъекты, которые с большей вероятностью будут причастны к деятельности по уклонению от уплаты налогов. Это особенно полезно, когда нет надежной информации, которая позволила бы идентифицировать соответствующих фигурантов. Выявление влиятельных членов преступной организации – одна из важнейших задач, которую берут на себя следователи по уголовным делам. Возможное решение – выявить наиболее значимых субъектов при помощи алгоритма центральности собственного вектора на основе матрицы смежности (Eigenvector Centrality) [22]. Оценка центральности (значимости) вершины пропорциональна сумме оценок всех вершин, соединенных с ней. Таким образом, если вершина соединена со многим значимыми вершинами, она также будет считаться значимой. Математически это можно выразить уравнением $Ax = \lambda x$, где A – матрица смежности с собственным значением λ (согласно теореме Перрона-Фробениуса

λ – наибольшее собственное значение матрицы смежности), x собственный вектор этой матрицы.

В рамках выше описанного примера, расследования уголовного дела по факту хищения бюджетных средств путем незаконного возмещения НДС с деятельности ООО Б. в особо крупном размере, решение об организаторе преступления и его исполнителях, сделано следователем с учетом информации о центральности указанных фигур в связи с большим количеством фактов хозяйственной деятельности ООО Б. по сравнению с иными потенциальными субъектами преступления: участие в создании ООО Б. и их аффилированных организаций, использованных в схеме преступления (из информации регистрационных дел налогового органа); представление интересов ООО Б. и аффилированных к нему организаций, участвующих в схеме преступления во взаимодействии с налоговыми органами (информация налогового органа по запросу следственного органа, анализ осмотра документов, изъятых в ходе обысков, выемок); участие в распоряжении денежными средствами ООО Б. и аффилированных к нему организаций, участвующих в схеме преступления (по данным юридических дел кредитных организаций); осуществление деятельности по адресу отправления налоговой отчетности по системе телекоммуникационной связи в налоговых орган (по данным налогового органа по IP-адресам отправки налоговой отчетности указанных организаций); наличие сведений о согласовании текущих вопросов деятельности ООО Б. и аффилированных к нему организаций, участвующих в схеме преступления (информация по результатам осмотров документов учета, изъятых в ходе обыска, выемок).

7. Поиск изоморфного подграфа

Многие реальные случаи уклонения от уплаты налогов реализуются посредством взаимодействия нескольких субъектов. Задача состоит в том, чтобы на основе сетевой онтологии, описывающей сетевые шаблоны подозрительной деятельности, извлекать топологическую информацию из комплексной сети, также известную как подграфы в анализе графов. Использование данного метода позволяет характеризовать, в частности, социальные связи, экономические взаимоотношения. Для примера приведём некоторые критерии аффилированности субъектов предпринимательской деятельности:

– участие одних и тех же лиц в создании, управлении организациями, в том числе через родственников или подконтрольных лиц;

– большая часть операций по расчетному счету приходится на взаимоотношения с аффилированной организацией;

– один адрес государственной регистрации.

Применения алгоритмов поиска сетевых шаблонов широко используется для выявления подозрительных групп при уклонении от уплаты налогов [23–27].

На основе используемой онтологии (рис. 3) сформулированы запросы на графовом языке запросов «Cypher». Используя данные запросы, можно, в частности, получить организации, связанные с интересующей организацией опосредованно. Данный алгоритм можно описать следующим образом:

1. указать интересующую организацию;
2. получить организации, связанные с интересующей организацией на удалении, например, до трех перемещений (прыжков);
3. для каждой организации, полученной на шаге 2, найти смежные вершины;
4. для каждого множества смежных вершин, полученных на шаге 3, вычислить коэффициент сходства Жаккарда с множеством смежных вершин интересующей организации.

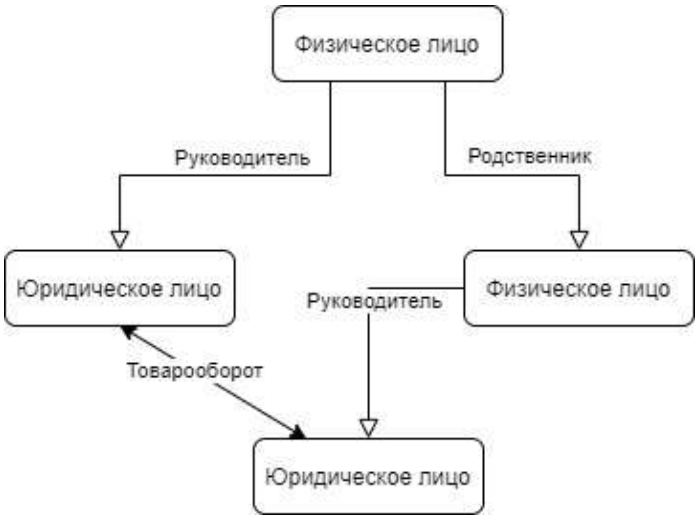


Рис. 3. Часть используемой онтологии
Fig. 3. Part of the ontology used

Коэффициент Жаккара (Jaccard Similarity) [28] в настоящее время является наиболее часто используемой мерой подобия в контексте анализа поведенческих связей, сходства между преступлениями. Привлекательность данного метода, отчасти, заключается в его простоте. Математически его можно выразить уравнением:

$$J = \frac{c}{a+b-c},$$

где a – множество смежных вершин интересующей организацией, b – множество смежных вершин организации (одной из), полученной на шаге 3 описанного выше алгоритма, c – пересечение этих множеств.

Применение данного алгоритма, в ходе расследования уголовного дела по факту уклонения от уплаты налогов с деятельности ООО Ж. в особо крупном размере путем необоснованного применения льготы по уплате НДС, позволило выявить признаки подконтрольности девяти организаций, формально не имеющих отношений к деятельности ООО Ж., однако, фактически с ним связанных. На основании информации, полученной из регистрирующего органа по результатам анализа документов регистрационных дел указанных организаций, установлено, что участниками указанных организаций являются лица, ранее являвшиеся административными работниками ООО Ж.; указанные организации также как и ООО Ж. имеют один адрес государственной регистрации; из информации, полученной из налогового органа установлено, что все организации имеют связь по месту осуществления бухгалтерского учета, формирования и направления налоговой отчетности; идентичными оказались и сведения о месте выхода в сеть по системе электронных расчетов Банк-Клиент всех указанных организаций, включая ООО Ж. Выявленные связи позволили сделать вывод о наличии подозрительной группы, состоящей из десяти субъектов (ООО Ж. и девять выше указанных организаций), использованных в преступной схеме.

Заключение

На примере расследования реальных уголовных дел продемонстрирована эффективность применения используемых алгоритмов в рассматриваемой предметной области. Показано, что использование алгоритмов сетевого анализа, таких как поиск изоморфного подграфа, предсказания связи, а также методов анализ социальных сетей, в частности определение наиболее значимых фигурантов, может способствовать значительному сокращению сроков расследования уголовного дела, выявить неочевидные/скрытые факты.

Предложенные алгоритмы позволяют анализировать собранную в рамках расследования информацию, включая сведения электронных баз данных учета налогоплательщика, данные электронных переписок, телефонных переговоров, соединений конкретных лиц, пр., позволяют при наличии межведомственного взаимодействия оперативно получать запрашиваемую информацию у различных источников (налоговые органы, органы внутренних дел, иные контрольные и правоохранительные органы), имеют существенное практическое значение для выявления и расследования налоговых преступлений, поскольку позволяют формировать схему налогового преступления, изменять ее с учетом новой криминалистической информации, обрабатываемой с применением информационных технологий, и на ее основе выдвинуть обоснованную и максимально достоверную в соответствии с установленным набором входных данных следственную версию события преступления.

СПИСОК ЛИТЕРАТУРЫ:

1. Bogahawatte K., Adikari S. 8th International Conference on Computer Science & Education. Intelligent criminal identification system, Colombo, Sri Lanka. 2013, p. 633–638. DOI: http://dx.doi.org/10.1109/ICCSE.2013.6553986.
2. Hamdy E., Adl A., Hassanien A.E., Hegazy O. and Kim T. -H. Criminal Act Detection and Identification Model, 2015 Seventh International Conference on Advanced Communication and Networking (ACN). 2015, p. 79–83. DOI: http://dx.doi.org/10.1109/ACN.2015.30.
3. Nath S.V. Crime Pattern Detection Using Data Mining, 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology Workshops. 2006, p. 41–44. DOI: http://dx.doi.org/10.1109/WI-IATW.2006.55.
4. Saravanan P., Selvaprabu J., Arun Raj L., Abdul Azeez Khan A., Javubar Sathick K. (2021) Survey on Crime Analysis and Prediction Using Data Mining and Machine Learning Techniques. In: Zhou N., Hemamalini S. (eds) Advances in Smart Grid Technology. Lecture Notes in Electrical Engineering, vol 688. Springer, Singapore. DOI: http://dx.doi.org/10.1007/978-981-15-7241-8_31.
5. Jihal H., Ounacer S., Ardchir S., Azouazi M. (2020) Clustering Model of False Positive Elimination in Moroccan Fiscal Fraud Detection. In: Ezziyyani M. (eds) Advanced Intelligent Systems for Sustainable Development (AI2SD'2019). Advances in Intelligent Systems and Computing, vol 1104. Springer, Cham. DOI: http://dx.doi.org/10.1007/978-3-030-36671-1_12.
6. Wu Y., Dong B., Zheng Q., Wei R., Wang Z. and Li X. A Novel Tax Evasion Detection Framework via Fused Transaction Network Representation, 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). 2020, p. 235–244. DOI: http://dx.doi.org/10.1109/COMPSAC48688.2020.00039.
7. Didimo W., Grilli L., Liotta G., Menconi L., Montecchiani F. and Pagliuca D. Combining Network Visualization and Data Mining for Tax Risk Assessment, in IEEE Access. Vol. 8, p. 16073–16086, 2020. DOI: http://dx.doi.org/10.1109/ACCESS.2020.2967974.
8. Taha K., Yoo P.D. Using the Spanning Tree of a Criminal Network for Identifying Its Leaders, in IEEE Transactions on Information Forensics and Security. Vol. 12, no. 2, p. 445–453, 2017. DOI: http://dx.doi.org/10.1109/TIFS.2016.2622226.
9. Zheng Q. et al. ATTENet: Detecting and Explaining Suspicious Tax Evasion Groups. «Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence». P. 6584–6586, 2019. DOI: http://dx.doi.org/10.24963/ijcai.2019/964.
10. Золотарёв О.В. и др., Система PullEnti – извлечение информации из текстов естественного языка и автоматизированное построение информационных систем. Ситуационные центры и информационно-аналитические системы класса 4i для задач мониторинга и безопасности, тр. межд. научн. конф., т. 2, ИФТИ, Протвино. 2016, с. 28–35. URL: https://www.elibrary.ru/item.asp?id=28185224 (дата обращения: 30 03 2021).
11. Announcing the Neo4j Crime Investigation Sandbox. URL: https://medium.com/neo4j/announcing-the-neo4j-crime-investigation-sandbox-c0c3bd9e71b1 (дата обращения: 30 03 2021).
12. Neo4j and the Offshore Leaks: the Case of Azerbaijan. URL: https://neo4j.com/graphgist/neo4j-and-the-offshore-leaks-the-case-of-azerbaijan (дата обращения: 30 03 2021).
13. Adamic L.A. и Adar E., Friends and neighbors on the web Social networks. Vol. 25, no. 3, p. 211–230, 2003. DOI: http://dx.doi.org/10.1016/S0378-8733(03)00009-1.

14. Zhou T., Lü L., Zhang Y.C. Predicting missing links via local information. The European Physical Journal. Vol. 71, no. 4, p. 623–630, 2009. DOI: http://dx.doi.org/10.1140/epjb/e2009-00335-8.
15. Barabâsi A.L. et al. Evolution of the social network of scientific collaborations. Physica A: Statistical mechanics and its applications. Vol. 311, no. 3-4, p. 590–614, 2002. DOI: http://dx.doi.org/10.1016/S0378-4371(02)00736-7.
16. Newman M.E.J. Clustering and preferential attachment in growing networks. Physical review. Vol. 64, no. 2, 2001. DOI: http://dx.doi.org/10.1103/PhysRevE.64.025102.
17. Martínez V., Berzal F., Cubero J C. A survey of link prediction in complex networks. ACM computing surveys (CSUR). Vol. 49, no. 4, p. 1–33, 2016. DOI: http://dx.doi.org/10.1145/3012704.
18. Rungsawang A., Manaskasemsak B. An Efficient Partition-Based Parallel PageRank Algorithm. Proceedings of the 11th International Conference Parallel and Distributed Computing, 2004. DOI: http://dx.doi.org/10.1109/ICPADS.2005.85.
19. Brandes U. A faster algorithm for betweenness centrality. Journal of mathematical sociology. Vol. 25, no. 2, p. 163–177, 2001. DOI: http://dx.doi.org/10.1080/0022250X.2001.9990249.
20. Sariyüce A.E., Kaya K., Saule E and Çatalyiirek Ü.V. Incremental algorithms for closeness centrality, 2013 IEEE International Conference on Big Data. 2013, p. 487–492. DOI: http://dx.doi.org/10.1109/BigData.2013.6691611.
21. Bihari A. and Pandia M.K. Eigenvector centrality and its application in research professionals' relationship network, 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE). 2015, p. 510–514. DOI: http://dx.doi.org/10.1109/ABLAZE.2015.7154915.
22. Li X. et al. Identifying social influence in complex networks: A novel conductance eigenvector centrality model. Neurocomputing. Vol. 210, p. 141–154, 2016. DOI: http://dx.doi.org/10.1016/j.neucom.2015.11.123.
23. Didimo W. et al. Visual querying and analysis of temporal fiscal networks. Information Sciences. Vol. 505, p. 406–421, 2019. DOI: http://dx.doi.org/10.1016/j.ins.2019.07.097.
24. Ruan J. et al. Identifying suspicious groups of affiliated-transaction-based tax evasion in big data. Information Sciences. Vol. 477, p. 508–532, 2019. DOI: http://dx.doi.org/10.1016/j.ins.2018.11.008.
25. Jihal H., Ounacer S., Ardchir S., Azouazi M. (2020) Clustering Model of False Positive Elimination in Moroccan Fiscal Fraud Detection. In: Ezziyyani M. (eds) Advanced Intelligent Systems for Sustainable Development (AI2SD'2019). Advances in Intelligent Systems and Computing, vol. 1104. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-36671-1_12.
26. Adamov A.Z. IEEE 13th International Conference on Application of Information and Communication Technologies (AICT). Machine Learning and Advanced Analytics in Tax Fraud Detection, 2019. DOI: http://dx.doi.org/10.1109/AICT47866.2019.8981758.
27. Stankevicius E., Leonas L. Hybrid approach model for prevention of tax evasion and fraud. Procedia-Social and Behavioral Sciences. Vol. 213, p. 383–389, 2015. DOI: http://dx.doi.org/10.1016/j.sbspro.2015.11.555.
28. Paul Jaccard. Etude comparative de la distribution florale dans une portion des Alpes et des Jura. Bulletin del la Socit Vaudoise des Sciences Naturelles, no. 37, p. 547–579. DOI: http://dx.doi.org/10.5169/seals-266450.

REFERENCES:

[1] Bogahawatte K., Adikari S. 8th International Conference on Computer Science & Education. Intelligent criminal identification system, Colombo, Sri Lanka. 2013, p. 633–638. DOI: http://dx.doi.org/10.1109/ICCSE.2013.6553986.
[2] Hamdy E., Adl A., Hassanien A.E., Hegazy O. and Kim T. -H. Criminal Act Detection and Identification Model, 2015 Seventh International Conference on Advanced Communication and Networking (ACN). 2015, p. 79–83. DOI: http://dx.doi.org/10.1109/ACN.2015.30.
[3] Nath S.V. Crime Pattern Detection Using Data Mining, 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology Workshops. 2006, p. 41–44. DOI: http://dx.doi.org/10.1109/WI-IATW.2006.55.
[4] Saravanan P., Selvaprabu J., Arun Raj L., Abdul Azeez Khan A., Javubar Sathick K. (2021) Survey on Crime Analysis and Prediction Using Data Mining and Machine Learning Techniques. In: Zhou N., Hemamalini S. (eds) Advances in Smart Grid Technology. Lecture Notes in Electrical Engineering, vol 688. Springer, Singapore. DOI: http://dx.doi.org/10.1007/978-981-15-7241-8_31.
[5] Jihal H., Ounacer S., Ardchir S., Azouazi M. (2020) Clustering Model of False Positive Elimination in Moroccan Fiscal Fraud Detection. In: Ezziyyani M. (eds) Advanced Intelligent Systems for Sustainable Development (AI2SD'2019). Advances in Intelligent Systems and Computing, vol 1104. Springer, Cham. DOI: http://dx.doi.org/10.1007/978-3-030-36671-1_12.
[6] Wu Y., Dong B., Zheng Q., Wei R., Wang Z. and Li X. A Novel Tax Evasion Detection Framework via Fused Transaction Network Representation, 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). 2020, p. 235–244. DOI: http://dx.doi.org/10.1109/COMPSAC48688.2020.00039.

[7] Didimo W., Grilli L., Liotta G., Menconi L., Montecchiani F. and Pagliuca D. Combining Network Visualization and Data Mining for Tax Risk Assessment, in IEEE Access. Vol. 8, p. 16073–16086, 2020. DOI: http://dx.doi.org/10.1109/ACCESS.2020.2967974.
[8] Taha K., Yoo P.D. Using the Spanning Tree of a Criminal Network for Identifying Its Leaders, in IEEE Transactions on Information Forensics and Security. Vol. 12, no. 2, p. 445–453, 2017. DOI: http://dx.doi.org/10.1109/TIFS.2016.2622226.
[9] Zheng Q. et al. ATTENet: Detecting and Explaining Suspicious Tax Evasion Groups. «Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence». P. 6584–6586, 2019. DOI: http://dx.doi.org/10.24963/ijcai.2019/964.
[10] Zolotarev O.V et al., System PullEnti — information extraction from natural language texts and automatic construction of information systems. School-Seminar (International) on Situational Centers and Information-Analytical System 4i Class for Monitoring and Security Tasks Proceedings, v. 2, IFTI, Protvino, 2016, p. 28–35. URL: https://www.elibrary.ru/item.asp?id=28185224 (accessed: 30 03 2021) (in Russian).
[11] Announcing the Neo4j Crime Investigation Sandbox. URL: https://medium.com/neo4j/announcing-the-neo4j-crime-investigation-sandbox-c0c3bd9e71b1 (accessed: 30 03 2021).
[12] Neo4j and the Offshore Leaks: the Case of Azerbaijan. URL: https://neo4j.com/graphgist/neo4j-and-the-offshore-leaks-the-case-of-azerbaijan (accessed: 30 03 2021).
[13] Adamic L.A. и Adar E., Friends and neighbors on the web Social networks. Vol. 25, no. 3, p. 211–230, 2003. DOI: http://dx.doi.org/10.1016/S0378-8733(03)00009-1.
[14] Zhou T., Lü L., Zhang Y.C. Predicting missing links via local information. The European Physical Journal. Vol. 71, no. 4, p. 623–630, 2009. DOI: http://dx.doi.org/10.1140/epjb/e2009-00335-8.
[15] Barabâsi A.L. et al. Evolution of the social network of scientific collaborations. Physica A: Statistical mechanics and its applications. Vol. 311, no. 3-4, p. 590–614, 2002. DOI: http://dx.doi.org/10.1016/S0378-4371(02)00736-7.
[16] Newman M.E.J. Clustering and preferential attachment in growing networks. Physical review. Vol. 64, no. 2, 2001. DOI: http://dx.doi.org/10.1103/PhysRevE.64.025102.
[17] Martínez V., Berzal F., Cubero J C. A survey of link prediction in complex networks. ACM computing surveys (CSUR). Vol. 49, no. 4, p. 1–33, 2016. DOI: http://dx.doi.org/10.1145/3012704.
[18] Rungsawang A., Manaskasemsak B. An Efficient Partition-Based Parallel PageRank Algorithm. Proceedings of the 11th International Conference Parallel and Distributed Computing, 2004. DOI: http://dx.doi.org/10.1109/ICPADS.2005.85.
[19] Brandes U. A faster algorithm for betweenness centrality. Journal of mathematical sociology. Vol. 25, no. 2, p. 163–177, 2001. DOI: http://dx.doi.org/10.1080/0022250X.2001.9990249.
[20] Sariyüce A.E., Kaya K., Saule E and Çatalyiirek Ü.V. Incremental algorithms for closeness centrality, 2013 IEEE International Conference on Big Data. 2013, p. 487–492. DOI: http://dx.doi.org/10.1109/BigData.2013.6691611.
[21] Bihari A. and Pandia M.K. Eigenvector centrality and its application in research professionals' relationship network, 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE). 2015, p. 510–514. DOI: http://dx.doi.org/10.1109/ABLAZE.2015.7154915.
[22] Li X. et al. Identifying social influence in complex networks: A novel conductance eigenvector centrality model. Neurocomputing. Vol. 210, p. 141–154, 2016. DOI: http://dx.doi.org/10.1016/j.neucom.2015.11.123.
[23] Didimo W. et al. Visual querying and analysis of temporal fiscal networks. Information Sciences. Vol. 505, p. 406–421, 2019. DOI: http://dx.doi.org/10.1016/j.ins.2019.07.097.
[24] Ruan J. et al. Identifying suspicious groups of affiliated-transaction-based tax evasion in big data. Information Sciences. Vol. 477, p. 508–532, 2019. DOI: http://dx.doi.org/10.1016/j.ins.2018.11.008.
[25] Jihal H., Ounacer S., Ardchir S., Azouazi M. (2020) Clustering Model of False Positive Elimination in Moroccan Fiscal Fraud Detection. In: Ezziyyani M. (eds) Advanced Intelligent Systems for Sustainable Development (AI2SD'2019). Advances in Intelligent Systems and Computing, vol. 1104. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-36671-1_12.
[26] Adamov A.Z. IEEE 13th International Conference on Application of Information and Communication Technologies (AICT). Machine Learning and Advanced Analytics in Tax Fraud Detection, 2019. DOI: http://dx.doi.org/10.1109/AICT47866.2019.8981758.
[27] Stankevicius E., Leonas L. Hybrid approach model for prevention of tax evasion and fraud. Procedia-Social and Behavioral Sciences. Vol. 213, p. 383–389, 2015. DOI: http://dx.doi.org/10.1016/j.sbspro.2015.11.555.
[28] Paul Jaccard. Etude comparative de la distribution florale dans une portion des Alpes et des Jura. Bulletin del la Socit Vaudoise des Sciences Naturelles, no. 37, p. 547–579. DOI: http://dx.doi.org/10.5169/seals-266450.

Поступила в редакцию – 31 октября 2021 г. Окончательный вариант – 01 марта 2022 г.
Received – October 31, 2021. The final version – March 01, 2022.

Якоб Я. Месенгисер[1], Марк А. Малахов[2], Наталья Г. Милославская[3]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: myy001@campus.mephi.ru, http://orcid.org/0000-0002-6674-4374
[2]e-mail: mma034@campus.mephi.ru, http://orcid.org/0000-0001-8599-1920
[3]e-mail: NGMiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

ЦЕНТРЫ УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ КАК СИЛЫ ГОССОПКА

DOI: http://dx.doi.org/10.26583/bit.2022.1.09

Аннотация. В статье рассматривается необходимость создания центра управления сетевой безопасностью (ЦУСБ), а также определяются функции ЦУСБ и требования к инфраструктуре на основании требований по обеспечению безопасности, предъявляемых к субъектам критической информационной инфраструктуры Российской Федерации (КИИ РФ). Целью настоящей работы является описание ЦУСБ как сил Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации (ГосСОПКА). В рамках работы решаются следующие задачи: определяется перечень контролирующих органов, регламентирующих процессы и меры обеспечения безопасности, предъявляемых к субъектам КИИ РФ для обеспечения безопасности объектов КИИ РФ, а также сами эти процессы и меры; описываются центры мониторинга безопасности и ЦУСБ как силы ГосСОПКА. Результаты настоящей работы можно использовать в рамках организации процессов взаимодействия с ГосСОПКА и создания ЦУСБ, занимающегося вопросами противодействия компьютерным атакам, обнаружения и реагирования на инциденты круглосуточно, и учебного курса, посвященного вопросам обеспечения безопасности объектов КИИ.

Ключевые слова: центр управления сетевой безопасностью, ГосСОПКА, КИИ РФ, компьютерная атака, информационная безопасность.
Для цитирования: МЕСЕНГИСЕР, Якоб Я.; МАЛАХОВ, Марк А.; МИЛОСЛАВСКАЯ, Наталья Г. ЦЕНТРЫ УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ КАК СИЛЫ ГОССОПКА. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 94–107, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1404. DOI: http://dx.doi.org/10.26583/bit.2022.1.09.

Yakob Y. Mesengiser[1], Mark A. Malakhov[2], Natalia G. Miloslavskaya[3]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31 Moscow, 115409, Russia
[1]e-mail: myy001@campus.mephi.ru, http://orcid.org/0000-0002-6674-4374
[2]e-mail: mma034@campus.mephi.ru, http://orcid.org/0000-0001-8599-1920
[3]e-mail: NGMiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

Network Security Centers as the GosSOPKA Forses

DOI: http://dx.doi.org/10.26583/bit.2022.1.09

Abstract. The paper addresses the need to create a Network Security Center (NSC), and the functions of the NSC and infrastructure requirements on the basis of security requirements imposed by the subjects of the critical information infrastructure (CII) of the Russian Federation (RF) to ensure the safety of CII objects of the RF. The current work describes the NSC as the forces of the State System for Detecting, Preventing and Eliminating the Consequences of Computer Attacks Aimed at the Information Resources of the RF (GosSOPKA). As part of the work, the following tasks are solved: a list of regulatory bodies regulating the processes and security measures presented to the subjects of the CII of the RF to ensure security of objects of the CII of the Russian Federation as well as these processes and measures themselves are determined; Security Operations Centers (SOCs) and NSCs as the GosSOPKA forces are described. It is possible to use the results obtained in the framework of the processes of organizing

cooperation with GosSOPKA, and the creation of a NSC dealing with computer attacks, detecting and responding to incidents around the clock; and a training course dedicated to the CII security.
Keywords: network security centers, GosSOPKA, critical information infrastructure of Russian Federation, computer attack, information security.
For citation: MESENGISER, Yakob Y.; MALAKHOV, Mark A.; MILOSLAVSKAYA, Natalia G. Network Security Centers as the GosSOPKA Forses. IT Security (Russia), [S.l.], v. 29, n. 1, p. 94–107, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1404. DOI: http://dx.doi.org/10.26583/bit.2022.1.09.

Введение

В настоящее время все сложнее становится противодействовать компьютерным атакам (КА). Так, за период с января по сентябрь 2019 г., удельный вес киберпреступлений, по данным МВД России, составил 13,5% [1]. В период с января по май 2021 г. удельный вес киберпреступлений вырос почти что до 27%[1] [2].

Угроза реализации КА актуальна и для органов власти, и для бизнеса, но для организаций, признанных субъектом критической информационной инфраструктуры Российской Федерации (КИИ РФ), КА представляют особую опасность для общества. Самостоятельно защищаться от таких атак способны далеко не все. 1 января 2018 г. вступил в силу Федеральный закон №187-ФЗ от 26.07.2017, который регулирует отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее КА[1]. Организациям, признанным субъектами КИИ РФ, необходимо обеспечить непрерывное и продуктивное взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации (ГосСОПКА)[2]. В рамках ГосСОПКА обеспечивается концентрация компетенций, необходимых для предотвращения КА и реагирования на них. При этом государство в лице Национального координационного центра по компьютерным инцидентам (НКЦКИ) выступает гарантом добросовестности центров ГосСОПКА, устанавливая требования к их деятельности, осуществляя надзор за этой деятельностью и даже непосредственно участвуя в реагировании на некоторые КА [3, 4].

Различные аспекты организации системы защиты объектов КИИ РФ рассматривались в публикациях [5–10]. В источнике [5] представлен исчерпывающий перечень документов, необходимых для разработки субъектами КИИ для создания и функционирования систем безопасности значимых объектов КИИ РФ. В [6] авторы предлагают фрагменты рекомендательной методики формирования требований к структурным подразделениям, необходимой для практического использования руководителями структурных подразделений ответственных за обеспечение безопасности значимых объектов КИИ РФ. В основе методики авторами была принята образовательная инициатива NICE, которая представляет собой сотрудничество правительства, научных кругов и частного сектора экономики, возглавляемое Национальным институтом стандартов и технологий Министерства торговли США [6]. В [7] авторами был представлен исчерпывающий состав мер по обеспечению безопасности объектов КИИ РФ третьей категории значимости. В [8] автор описывает способы взаимодействия объектов топливно-энергетического комплекса с ГосСОПКА. Так, сообщение об инциденте может быть передано через интернет-портал НКЦКИ, письмом по электронной почте,

[1]МВД России публикует данные о состоянии преступности по итогам пяти месяцев 2021 года. URL: https://мвд.рф/news/item/24738876 (дата обращения: 01.01.2022).

[2]Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: https://docs.cntd.ru/document/436752114/ (дата обращения: 01.01.2022).

телефонным звонком или официальным письмом. Также возможна передача сведений об инциденте с помощью специальных средств взаимодействия, напрямую подключающихся к инфраструктуре НКЦКИ. Возможна и следующая схема взаимодействия: субъект КИИ, обслуживаемый центром ГосСОПКА, может сообщить об инциденте в этот центр ГосСОПКА, и оно будет передано в НКЦКИ [8]. При организации системы защиты объектов КИИ РФ следует уделять должное внимание курсам повышения квалификации сотрудников. Так, в [9] автором рассматривается программа повышения квалификации, позволяющая слушателям курса получить знания и навыки в области обеспечения безопасности объектов КИИ РФ. Программа разъясняет действия государственных органов, учреждений и других организаций при реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В [10] авторами был представлен сравнительный анализ подходов к категорированию объектов КИИ в РФ и США. В работе рассматриваются основные законы, регулирующие вопросы обеспечения безопасности объектов КИИ в РФ и США, области КИИ в РФ и США. Приводится сравнение областей КИИ. Также рассматриваются основные методы по категорированию критической инфраструктуры в РФ и США. На основании проведенного исследования авторами делается вывод о схожести в выделении областей КИИ в РФ и США и принципиальных различиях в методиках соблюдения безопасности КИИ.

Таким образом, проведенный выше небольшой обзор научных статей показывает, что организация эффективного и результативного противодействия КА является актуальной темой: авторы работ раскрывают различные аспекты защиты объектов КИИ РФ. В рамках настоящей работы авторы предлагают описание подразделения – центра управления сетевой безопасностью (ЦУСБ), способного обеспечить эффективность и результативность противодействия КА. ЦУСБ также ответственен за информирование и взаимодействие с центром ГосСОПКА. Первоочередной целью развертывания ЦУСБ [11] является предоставление организации возможностей по организации непрерывных процессов предотвращения, выявления и оперативного реагирования на события и инциденты, происходящие в реальном времени, а также по прогнозированию и предупреждению КА на защищаемые объекты КИИ РФ на всех стадиях их жизненного цикла на основе своевременного анализа данных об этих событиях и инцидентах.

Таким образом, являясь частью субъекта КИИ РФ, ЦУСБ может выступать в роли силы ГосСОПКА. Целью данной статьи является определение функций ЦУСБ и требований к инфраструктуре на основании требований по обеспечению безопасности, предъявляемых к субъектам КИИ РФ.

1. Перечень контролирующих органов, регламентирующих правила, процессы и меры обеспечения безопасности для объектовКИИ РФ

Одним из важнейших этапов в области обеспечения безопасности КИИ РФ, согласно Федеральному закону №187-ФЗ, является создание ГосСОПКА.

ГосСОПКА включает в себя силы и средства. Федеральный закон №187-ФЗ относит к силам ГосСОПКА следующие субъекты:

1) подразделения и должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования ГосСОПКА на информационные ресурсы РФ. В соответствии с указом Президента РФ от 15.01.2013

№31с этим органом является Федеральная Служба Безопасности Российской Федерации (ФСБ России)[3]. Функции ФСБ России определены в федеральном законе №187-ФЗ[1].

2) организация, создаваемая федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования ГосСОПКА на информационные ресурсы РФ, для обеспечения координации деятельности субъектов КИИ РФ по вопросам обнаружения, предупреждения и ликвидации последствий КА и реагирования на компьютерные инциденты – НКЦКИ[1]. Важно отметить, что согласно Федеральному закону №187-ФЗ, НКЦКИ осуществляет свою деятельность в соответствии с положением, утверждаемым ФСБ России[1]. Содержание положения ФСБ России о деятельности НКЦКИ представлено в приказе ФСБ России от 24 июля 2018 г. №366[4];

3) подразделения и должностные лица субъектов КИИ РФ, которые принимают участие в обнаружении, предупреждении и ликвидации последствий КА и в реагировании на компьютерные инциденты[1].

Также следует отметить указ Президента РФ от 25.11.2017 №569[4], в котором Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченный орган в области экспортного контроля.

2. Процессы и меры обеспечения безопасности объектов КИИ РФ

Для определения процессов и мер обеспечения безопасности объектов КИИ РФ необходимо определить категорию значимости рассматриваемых объектов КИИ РФ. Определять категорию значимости объектов КИИ РФ следует согласно постановлению Правительства РФ от 8 февраля 2018 г. №127[5]. После определения категории значимости объектов КИИ РФ возможно переходить к выбору процессов и мер обеспечения безопасности объектов КИИ РФ, руководствуясь приказом ФСТЭК России от 25 декабря 2017 г. №239[6]. В этом документе определены следующие группы мер обеспечения безопасности объектов КИИ РФ в соответствии с категорией значимости этих объектов:

- идентификация и аутентификация;
- управление доступом;
- ограничение программной среды;
- защита машинных носителей информации;
- аудит безопасности;
- антивирусная защита;
- предотвращение вторжений (компьютерных атак);
- обеспечение целостности;

[3]Указ Президента РФ от 15.01.2013 №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». URL: https://docs.cntd.ru/document/902392496 (дата обращения: 01.01.2022).

[4]Приказ ФСБ России от 24 июля 2018 г. №366 «О Национальном координационном центре по компьютерным инцидентам». URL: https://publication.pravo.gov.ru/Document/View/0001201809100001 (дата обращения: 01.01.2022).

[5]Постановление Правительства РФ от 8 февраля 2018 г. №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». URL: https://docs.cntd.ru/document/556499040 (дата обращения: 01.01.2022).

[6]Приказ ФСТЭК России от 25 декабря 2017 г. №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». URL: http://publication.pravo.gov.ru/Document/View/0001201803270041 (дата обращения: 01.01.2022).

- обеспечение доступности;
- защита технических средств и систем;
- защита информационной (автоматизированной) системы и ее компонентов;
- реагирование на компьютерные инциденты;
- управление конфигурацией;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению безопасности;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

В приказе ФСБ России от 6 мая 2019 г. №196 представлены требования к средствам ГосСОПКА, средствам обнаружения, предупреждения и ликвидации последствий, средствам технические, программные, программно-аппаратные и иные средства поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ, средствам обмена и криптографическим средствам защиты информации, необходимой субъектам КИИ РФ в части реализации функций безопасности, визуализации, построения сводных отчетов и хранения информации[7].

Схематическое представление связи терминов и определений, представленных в нормативных правовых документах[2-7], приведено на рис. 1.

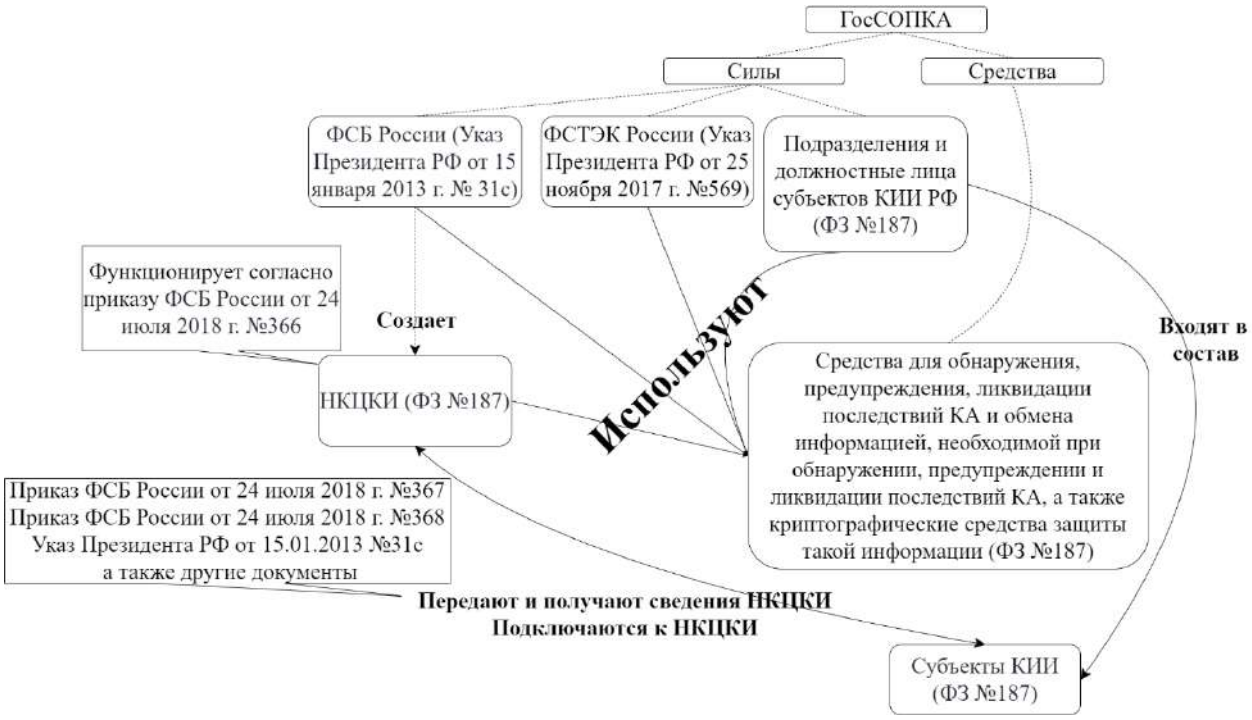


Рис. 1. Схематическое представление связи терминов и определений, представленных в нормативных правовых документах[2-7]
Fig. 1. Visual representation of the connection between terms and definitions presented in the regulatory legal documents[2-7]

[7]Приказ ФСБ России от 6 мая 2019 г. №196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты». URL: https://docs.cntd.ru/document/554691438 (дата обращения: 01.01.2022).

3. ЦМБ как силы ГосСОПКА, их функции и требования к инфраструктуре

Задача автоматизации работ по обработке информации и событий информационной безопасности (ИБ) заключается в создании организацией собственного специализированного подразделения – центра мониторинга безопасности (ЦМБ) [12].

С организационной точки зрения ЦМБ – это централизованное подразделение, которое занимается вопросами мониторинга ИБ на организационном уровне, а также плюс созданная для обнаружения, анализа, подготовки отчетности и реагирования на инциденты ИБ группа, состоящая в основном из операторов, работающих с текущими данными, и аналитиков безопасности, которые выполняют углубленный анализ собранных данных[8]. Аналитики безопасности осуществляют анализ ранее не происходивших и неизвестных событий ИБ и новых уязвимостей, опираясь на различные источники и исторические данные самой организации (в случае ЦМБ срок давности таких данных обычно составляет от нескольких дней до месяца). У них должно быть четкое понимание локальной, региональной и глобальной среды и событий, которые могут повлиять на безопасность функционирования информационно-телекоммуникационных сетей (ИТКС) субъектов КИИ РФ и, как следствие, деятельности организации в целом. Штат ЦМБ зависит от сложности ИТКС организации.

С технической точки зрения – это детально разработанные процессы мониторинга ИБ ИТКС с предопределенными процедурами реагирования в конкретных ситуациях и взаимодействия с различными подразделениями внутри самой организации и другими структурами (в случае необходимости), а также арсенал специализированных средств для автоматизации такой деятельности

ЦМБ исключает потребность вручную искать, собирать, оценивать, классифицировать, анализировать и, в конечном счете, дифференцировать и связывать с ИБ данные, полученные из многочисленных гетерогенных источников в ИТКС организации[9]. Он непрерывно контролирует безопасность сетей, анализирует локально и дистанционно эксплуатируемые злоумышленниками уязвимости элементов ИТКС и может рассматриваться как ядро обеспечения сетевой безопасности в рамках ИТКС на операционном уровне управления сетью. ЦМБ как основа для осуществления дальнейшей деятельности по реагированию на инциденты ИБ централизованно собирает данные с сотен средств защиты информации (СЗИ) и обобщает их в единую картину состояния сетевой безопасности ИТКС, помогая персоналу ЦМБ быстро разобраться в текущей ситуации. Чтобы обеспечивать эти качества, ЦМБ в ИТКС должен работать в круглосуточном режиме и выполнять следующие типовые функции [13]:

- эксплуатационная поддержка функционирования ЦМБ с командной консолью, используемой для выполнения различных команд расширенного администрирования (повседневной эксплуатации и управления), поиска неисправностей и решения возникающих проблем силами самого субъекта КИИ РФ;
- отслеживания состояния активов ИТКС для их последующего восстановления после инцидентов ИБ;
- идентификация на основе результатов сканирования уязвимостей для последующего управления установкой обновлений для устранения найденных уязвимостей;

[8]Security Operations Center. 2015. URL: http://resources.infosecinstitute.com/security-operations-center/ (дата обращения: 30.12.2021).

[9]Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press, 2015. URL:https://supportforums.cisco.com/sites/default/files/security_operations_center_9780134052014_ch_1_final__0.pdf (дата обращения: 30.12.2021).

● анализ сетевого трафика и информации о потоках данных для поиска любых сведений, которые могут быть полезны для выявления неисправностей и отклонений от штатного функционирования всех элементов ИТКС и, в конечном счете, обнаружения событий ИБ;

● мониторинг устройств и связь с системами управления их конфигурированием и централизованного управления СЗИ, предназначенными для автоматизации и полного контроля их жизненного цикла, включая единое управление процессами конфигурирования, настройки политик, оценки статуса, генерации отчетов о функционировании и т.д.;

● управление информацией о безопасности на основе сбора журналов регистрации событий (ЖРС), их хранения, архивирования и подготовки соответствующей отчетности, используемой далее для управления рисками ИБ и их ранжирования на основе анализа воздействия на бизнес, включая пассивную оценку и активную обработку рисков ИБ;

● обработка данных о событиях/инцидентах ИБ с непрерывной обратной связью и, при необходимости, эскалацией проблем на высшие уровни в организации;

● осуществление действий по сбору свидетельств компьютерных преступлений для реконструкции инцидента ИБ в ИТКС в признаваемом при судебном расследовании порядке, включая идентификацию, сбор, сохранение, восстановление, анализ и представление фактов.

Средства, которые должны использоваться для обеспечения работы ЦМБ (а, значит, и ЦУСБ) в достаточной мере описаны в Приказе Федеральной службы безопасности Российской Федерации от 06.05.2019 № 196[7].

Традиционные ЦМБ, работающие на основе правил, хорошо справлялись с задачей защиты от традиционных атак несколько лет назад. В настоящее время ИТКС как единое целое часто не является конечной целью злоумышленников; наоборот, их интересуют конечные устройства, поскольку ценные данные часто находятся именно там. Атаки характеризуются большей целенаправленностью, продуманностью, подготовленностью, использованием скрытых технологий взлома (например, APT-атаки и атаки на стороне клиента). Можно сделать вывод, что первые ЦМБ не были рассчитаны на растущие объемы данных, относящихся к ИБ современных гетерогенных ИТКС, и им не удавалось сохранять полный контроль над сложной сетевой ситуацией и поддерживать требуемый уровень ИБ ИТКС должным образом.

На основе анализа первоисточников, описывающих практический опыт внедрения и использования ЦМБ, были выявлены следующие серьезные ограничения их функциональных возможностей [14]:

● невозможность работы в крупномасштабных, гетерогенных, распределенных и сложно связанных ИТКС с подключением пользователей из любого места в любое время;

● ручная интеграция различных технологий защиты в едином ЦМБ;

● недостаточная гибкость и производительность ЦМБ для обработки больших объемов ранее накопленных (исторических), только что собранных и аналитически выведенных на их основе данных, известных как «технологии больших данных»;

● невозможность обеспечить высокую степень надежности/устойчивости при сборе, передаче и обработке данных о событиях ИБ, что делает их уязвимыми к атакам на SIEM-систему и сам ЦМБ;

● зависимость от централизованных правил корреляции, обрабатываемых на одном узле, что затрудняет масштабируемость, создает уязвимости и единую точку отказа;

● ограниченные возможности анализа, оценки и визуализации уровня ИБ, поскольку ЦМБ осуществляет мониторинг событий на сетевом уровне и поиск неисправностей во внутренних элементах ИТКС, а также обеспечивает не очень сложную корреляцию;

● невозможность интерпретации данных более высоких уровней, таких как данные об услугах или деятельности;

● отсутствие реакции на выявленные атаки в режиме реального времени; в дополнение к автоматизированным операциям аналитики ЦМБ должны оценивать в режиме реального времени большие объемы данных, что практически не осуществимо, и далее вручную реагировать на них.

На основе этих недостатков можно сформулировать требования к более функциональным, чем ЦМБ, ЦУСБ ИТКС организации, среди которых ключевыми являются следующие [11]:

● максимальная автоматизация рутинных операций не только по мониторингу ИБ, но и полноценному управлению инцидентами ИБ в ИТКС, приближающая реагирование на инциденты ИБ к режиму реального времени и по возможности предотвращающая их возникновение;

● создание полной видимости происходящего в ИТКС;

● анализ не только состояния, но и поведения всех элементов ИТКС и ее пользователей в определенном контексте для немедленного выявление отклонений по сравнению с нормальным поведением или функционированием, а не просто обнаружение на основе сигнатур, которые требуется постоянно обновлять и пополнять;

● поддержание требуемого организацией уровня ИБ в ИТКС в течение длительного времени без необходимости обращения к экспертам.

4. ЦУСБ как силы ГосСОПКА, их функции и требования к инфраструктуре

Центр управления сетевой безопасностью (ЦУСБ) является естественной эволюцией традиционного ЦМБ. Он решает проблемы ЦМБ путем объединения ЦМБ и концепции – интеллектуальной безопасности. Концепция интеллектуальной безопасности нашла свое воплощение в центре полноценного управления (а не просто мониторинга) ИБ ИТКС организации второго поколения – центре интеллектуальной безопасности (ЦИБ). Он имеет интегрированную архитектуру защиты от КА и объединяет полную прозрачность и контекстно-управляемый интеллект с действенным и всеобъемлющим пониманием и управлением знаниями в области ИБ[10], что позволяет постоянно контролировать ИБ ИТКС и связанных с ней элементов единого информационного пространства (ЕИП) организации. Внедряя ЦИБ, организация получает целостный и глубокий детальный взгляд на «здоровье» своей ИТКС и возможность не только обнаруживать и реагировать на атаки, но и результативно бороться с новыми угрозами ИБ, прежде чем они причинят вред, а также предотвращать инциденты ИБ, постоянно собирая и обобщая знания о сетевых атаках и уязвимостях в контексте конкретной ИТКС [9]. В России ЦИБ, использующий искусственный интеллект, был создан, например, в ПАО «Сбербанк России», в 2016 г., в результате чего количество рассматриваемых в день подозрительных событий в работе систем увеличилось до нескольких миллионов (до создания ЦИБ банку удавалось проанализировать лишь 100–200 инцидентов в день) [11].

[10]SOC vs. SIC: The Difference of an Intelligence Driven Defense® Solution. A White Paper. ITSECURITYNEWS. – Lockheed Martin Corporation, 2015. URL: https://www.itsecuritynews.info/soc-vs-sic-the-difference-of-an-intelligence-driven-defense-solution/ (дата обращения: 30.12.2021).

Как комплексное решение, ЦИБ с ИБ-аналитикой применительно к ИТКС организации в полном объеме сочетает в себе ряд интегрированных в единое целое технологий, а именно [14]:

- управление знаниями в области ИБ и содействие применению комплексного подхода к выявлению, сбору, оценке, поиску и обмену этими знаниями;
- обработка больших относящихся к ИБ данных в определенном контексте – с точки зрения любой возможной атаки для нахождения ее источника, установления ее типа, оценки последствий, визуализации направленности, выявления всех затронутых систем, приоритезации мер обеспечения ИБ и выработки предложений по нейтрализации последствий атаки;
- идентификация, отслеживание и восстановление всех элементов ИТКС после воздействия на них различных инцидентов ИБ;
- сбор данных из гетерогенных источников и управление ЖРС и учетными записями с учетом соблюдения соответствия определенным требованиям;
- централизация и агрегирование данных из разрозненных хранилищ с последующей нормализацией, корреляцией, категоризацией и анализом с применением SIEM-систем;
- визуализация уровня ИБ ИТКС и усовершенствованное (без использования статически заданных правил) обнаружение вторжений для выявления аномалий в поведении сети;
- управление рисками ИБ, сокращающее число инцидентов ИБ и обеспечивающее выполнение требований по обеспечению ИБ;
- весь цикл обработки инцидентов ИБ, заключающийся в обнаружении, оповещении, предоставлении отчетности, реагировании (включая антикризисные действия) и управлении эскалацией проблем на высшие уровни для принятия решений;
- сканирование уязвимостей с последующей реконфигурацией устройств и управлением изменениями и обновлениями;
- анализ сетевого трафика и приложений, поддерживаемый межсетевыми экранами следующего поколения (NGFW) и инструментами для расследования инцидентов ИБ.

Со своим ЦИБ организация может реализовать персонифицированное (индивидуальное) в контексте ее деятельности управление инцидентами ИБ для ИТКС. Образно говоря, если ЦМБ – это «глаза мониторинга инцидентов ИБ», то ЦИБ – это «мозг управления инцидентами ИБ с широко открытыми глазами» [15], поскольку при осуществлении управления инцидентами ИБ собранные данные о реальном уровне ИБ всей ИТКС и ее отдельных элементов и принятые обоснованные решения по корректировке этого уровня должны использоваться для реагирования на инциденты ИБ.

Учитывая все ранее выявленные возможности и ограничения ЦМБ и ЦИБ, можно определить основные характеристики ЦУСБ, который:

- функционирует на основе сценариев инцидентов ИБ и моделирования процесса «охоты за угрозами»;
- способен обнаруживать не только типовые и целенаправленные атаки, но и усложненные угрозы ИБ и атаки «нулевого дня»;
- производит обнаружение на основе разработки сценариев, исторических данных, машинного обучения и «охоты за угрозами», а также агрегированных внутренних и внешних потоков;

- реагирует упреждающее, в основном автоматизированное реагирование за счет автоматизации выполнения критически важных задач на основе специальных программных модулей (скриптов);
- сопровождает инциденты ИБ на протяжении всего заранее смоделированного периода его развития с постоянной коррекцией и настройкой поиска связанных с инцидентом данных в зависимости от получаемых результатов его расследования;
- устанавливает время реагирования на инциденты ИБ в документах и в реальности зависящее от его последствий, включая время, требуемое на коррекцию поиска связанных с инцидентом данных;
- состоит из специализированных лабораторий для разработки сценариев инцидентов и выполнения тестирования защищенности;
- орудует средствами расширенного поиска, агрегирования данных от всех источников и управления ими;
- дополнительно имеет в распоряжении специализированные средства для обнаружения угроз ИБ, поиска данных и реализации сценариев детального целенаправленного исследования угроз ИБ (Threat Hunting);
- работает постоянно в режиме реального/близкого к реальному времени обнаружения и реагирования;
- состоит из персонала, обладающего навыками моделирования и глубокого анализа корреляций всех собираемых данных и коррекций поиска новых данных;
- осуществляет визуализацию в режиме «жесткого» реального времени.

Следовательно, для того, чтобы соответствовать данным характеристикам, деятельность ЦУСБ должна определяться, но не ограничиваться следующими общими требованиями:

1. Вся деятельность ЦУСБ организации должна быть выстроена и реализована согласно требованиям, изложенным в применимых нормативных, правовых, отраслевых и других документах.
2. ЦУСБ должен представлять собой комплекс систем (подсистем), технических и программных средств, технологически и организационно объединенных каналами передачи информации различной физической природы, позволяющих обеспечить автоматизацию процесса управления инцидентами информационной безопасности (ПУИИБ) организации, включая реагирование на инциденты ИБ, за счет централизованной обработки связанной с ИБ ИТКС информации, а также предоставляющий услуги и средства связи для персонала, вовлеченного в ПУИИБ.
3. Единство и скоординированность функционирования ЦУСБ с ИТКС организации.
4. ЦУСБ должен быть системообразующим элементом системы обеспечения ИБ организации на основе жесткой связи с ней, влиять на ее развитие и совершенствование.
5. Наличие необходимой организационной структуры и органа управления ЦУСБ, основными задачами которого является администрирование управления, управление ходом функциональных процессов, оперативный контроль состояния, оперативный контроль над устранением сбоев в функционировании и информационно-аналитическое обеспечение управления совершенствованием и развитием ЦУСБ.
6. Интеграция информационных и телекоммуникационных сетей, ресурсов и услуг ЦУСБ в единую систему.
7. Применение современных средств технического, программного, информационного, аналитического, организационного и документального обеспечения, функционально объединенных в ЦУСБ.

Вышеуказанные требования являются отправной точкой для развития ЦУСБ, однако для совершенствования его функционирования предлагается использовать также и специальные требования:

1. Создание и непрерывное развитие ЦУСБ как единой экосистемы (сложной динамической системы взаимосвязанных элементов в ЕИП организации, а не просто единой платформы) для обмена информацией об ИБ ИТКС и совместных скоординированных действий по обнаружению, расследованию и предотвращению инцидентов ИБ, а также упреждающего управления сетевой безопасностью ИТКС и обучения на полученном опыте как различных подразделений организации, так и ее бизнес-партнеров, регуляторов, аудиторов и т.п.

2. Управляемость ЦУСБ с централизованной архитектурой и распределенной/ децентрализованной работой отдельных процессов при совмещении масштабируемости и эластичности сбора, хранения, первичной обработки и корреляции данных для его функционирования в изменяющейся среде осуществления деятельности организации и при появлении новых угроз ИБ в ЕИП для ее ИТКС.

3. Согласованность процессов, поддерживающих функционирование ЦУСБ, со всеми передовыми практиками и применимыми к ИТКС организации требованиями по обеспечению ИБ, определенными в международных и российских законах и подзаконных нормативных правовых актах, а также региональными и ведомственными документами.

4. Расширенная ИБ-аналитика и использование для нее как можно большего количества типов данных, поскольку по-прежнему недостаточно навыков и методов обработки неструктурированных данных в состоянии покоя, например данных из ОЗУ конечных устройств, данных от мобильных устройств, виртуальных и облачных сред.

5. Адаптивное управление событиями ИБ в ИТКС, поддерживаемое за счет применения предсказательного определения возможных тенденций в области обеспечения ИБ в ЕИП организации и типовых модульных и конфигурируемых СЗИ, сетевых устройств, протоколов, процессов и мер обеспечения сетевой безопасности, что должно обеспечить повторяемость (тиражируемость) всех процессов управления сетевой безопасностью при их использовании в различных ЦУСБ.

6. Функциональная устойчивость ЦУСБ в штатном режиме, в условиях направленных на него КА, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций (способность регулировать функционирование с целью поддержания выполнения операций при ожидаемых условиях и при ужесточении требований, нарушениях и непредвиденных обстоятельствах, например, способность адаптироваться к изменяющимся шаблонам компьютерных атак или условиям осуществления деятельности на основе ИТКС при внедрении новых ИКТ [16]) для обеспечения долгосрочной постоянной доступности и других важных свойств ИБ для ИТКС и всех ее элементов, аппаратного (АО) и программного обеспечения, предоставляемых ИТ-услуг, информационных потоков, знаний и баз данных и т.д., что исключит единую точку отказа.

7. Масштабируемость ЦУСБ (мера способности ИТКС к увеличению/уменьшению производительности и затрат в ответ на изменения в его потребностях в АО, приложениях, системах обработки данных и т.п.[11]) для сбора и обработки огромного количества событий из различных гетерогенных внутренних и внешних (типа Threat Intelligence) по отношению к ИТКС источников, что все вместе определяет необходимость

[11]IT Glossary. GARTNER. URL: https://blogs.gartner.com/it-glossary/operational-resilience/ (дата обращения: 30.12.2021).

применения ИТ больших данных и использования продвинутых технологий для их хранения.

8. Эластичность (способность системы с течением времени увеличивать нагрузку на свои текущие и дополнительные динамически и автоматически добавляемые по требованию вычислительные ресурсы[12]) для распределенных и реализуемых в режиме реального/близкого к реальному времени агрегирования, пакетной и потоковой обработки и передачи гибридных относящихся к ИБ больших данных.

9. Гибкость при использовании необходимых методов и инструментов ИБ-аналитики таким образом, чтобы персонал ЦУСБ мог использовать при обработке все доступные в тот момент данные (включая исторические за длительный период времени) и получать результаты, учитывающие разные точки зрения.

10. Собственная защищенность и надежность ЦУСБ, включая защищенность его инфраструктуры и процессов обработки данных, а также безопасность всех обрабатываемых в нем связанных с ИБ больших данных и хранимых входные и выходные данных процессов, а также надежность управления, поступающими в ЦУСБ из надежных источников.

11. Прозрачность для руководства организации всей деятельности ЦУСБ для принятия своевременных управленческих решений.

Заключение

В данной работе ЦУСБ описаны как силы ГосСОПКА, определены функции ЦУСБ и требования к его инфраструктуре в соответствии с требованиями, предъявляемыми субъектам КИИ РФ для обеспечения безопасности объектов КИИ РФ.

Полученные результаты позволят не только наладить взаимодействия с центром ГосСОПКА в соответствии с требованиями законодательства РФ, но и помогут специалистам информационной безопасности в построении организационного объекта, который может заниматься вопросами противодействия компьютерным атакам, обнаружении и реагировании на инциденты круглосуточно в единой централизованной системе с возможностью непрерывного развития как самого ЦУСБ, так и его интегрированности в процессы и инфраструктуру организации.

Кроме того, с применением указанных основных и дополнительных требований, имеется возможность проведения дальнейших исследований для определения структуры ЦУСБ, его программно-аппаратного обеспечения

Предложенные требования являются начальными и могут быть дополнены при их внедрении для обеспечения безопасности объектов КИИ РФ на достаточном с точки зрения нормативных документов РФ по данному вопросу.

СПИСОК ЛИТЕРАТУРЫ:

1. Лобач Д.В., Смирнова Е.А. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам. Территория новых возможностей. Вестник Владивостокского Государственного Университета Экономики и Сервиса. Т. 11, № 4, с. 23–32, 2019. DOI: http://dx.doi.org/10.24866/VVSU/2073-3984/2019-4/023-032.
2. Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства. Государственное управление. Электронный вестник. № 89, с. 184–196, 2021. DOI: http://dx.doi.org/10.24412/2070-1381-2021-89-184-196.

[12]Cyber Security: Security Operations Center (SOC) vs. Network Operations Center (NOC). INTELLECTUALPOINT. 2016. URL: https://www.intellectualpoint.com/blog/cyber-security-security-operations-center-soc-vs-network-operations-center-noc/ (дата обращения: 30.12.2021).

3. Ванцева И.О., Зырянова Т.Ю., Медведева О.О. Влияние федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» на владельцев критических информационных инфраструктур. Вестник УРФО. Безопасность в информационной сфере. № 4, с. 71–76, 2018. ISSN 2225-5435. URL: http://info-secur.ru/is_1_2018.pdf. (дата обращения: 01.01.2022).
4. Деева Т.В. Создание единой системы противодействия кибератакам: ответ на большие вызовы и угрозы налоговой безопасности страны. Проблемы рыночной экономики. № 4, с. 100–112, 2020. ISSN 2500-2325. URL: https://www.elibrary.ru/item.asp?id=44682826 (дата обращения: 08.01.2022).
5. Заворина Л.Д., Селифанов В.В. Разработка системы защиты информации значимого объекта критической инфраструктуры Российской Федерации. Сборник научных трудов Новосибирского Государственного Технического Университета. № 1, с. 123–131, 2018. ISSN 2307-6879. URL: https://www.elibrary.ru/item.asp?id=39157958. (дата обращения: 08.01.2022).
6. Гавдан Григорий П., Иваненко Виталий Г., Салкуцан Алексей А. Обеспечение безопасности значимых объектов КИИ. Безопасность информационных технологий, [S.l.], т. 26, № 4, с. 69–82, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.05.
7. Зырянова Т.Ю. Анализ требований третьей категории значимости объектов КИИ в инфраструктуре предприятия. Вестник УРФО. Безопасность в информационной сфере. № 3, с. 69–72, 2019. ISSN 2225-5435. URL: https://www.elibrary.ru/item.asp?id=41151823 (дата обращения: 08.01.2022).
8. Козьминых С.И. Взаимодействие объектов топливно-энергетического комплекса с ГосСОПКА. Информационные ресурсы России. № 1, с. 2–7, 2020. ISSN 0204-3653. URL: https://www.elibrary.ru/item.asp?id=42512104 (дата обращения: 08.01.2022).
9. Каннер Татьяна М. Особенности повышения квалификации специалистов по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 26, № 3, с. 22–31, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.3.02 (дата обращения: 01.01.2022).
10. Кузнецов С.А., Куликов И.А., Фоминых А.А. Сравнение КИИ и методов категорирования КИИ в РФ и США. Актуальные научные исследования в современном мире. № 6–1, с. 63–68, 2021. ISSN 2524-0986. URL: https://www.elibrary.ru/item.asp?id=46326396 (дата обращения: 08.01.2022).
11. Милославская Н.Г. Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. М.: Горячая линия-Телком. 2020. – 461 с.
12. Bidou Renaud. Security Operation Center Concepts & Implementation. 2005. URL: http://iv2-technologies.com/~rbidou/SOCConceptAndImplementation.pdf (дата обращения: 30.12.2021).
13. Наташова Кристина В. и др. К вопросу о категорировании объектов критической информационной инфраструктуры морских портов. Безопасность информационных технологий, [S.l.], т. 27, № 2, с. 35–46, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.2.03.
14. Miloslavskaya Natalia G. Information Security Management in SOCs and SICs. Journal of Intelligent & Fussy Systems. Vol. 35, no. 3, p. 2637–2647, 2016. ISBN 1875-8967. URL: https://www.elibrary.ru/item.asp?id=38633644 (дата обращения: 09.01.2022).
15. Милославская Наталья Г. Центры управления информационной безопасностью. Безопасность информационных технологий, [S.l.], т. 23, № 4, с. 38–51, 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/257 (дата обращения: 09.01.2022).
16. Лебедев Павел. Сбербанк обезопасит себя с помощью искусственного интеллекта. 2016. URL: https://banks.cnews.ru/news/top/2016-06-10_sberbank_obezopasit_sebya_s_pomoshchyu_iskusstvennogo (дата обращения: 30.12.2021).

REFERENCES:

[1] Lobach D.V., Smirnova E.A. The state of cybersecurity in Russia at the present stage of the digital transformation of society and the formation of a national system for countering cyber threats. A territory of new opportunities. Vladivostok State University of Economics and Service Bulletin. Vol. 11, no. 4, p. 23–32, 2019. DOI: http://dx.doi.org/10.24866/VVSU/2073-3984/2019-4/023-032 (in Russian).
[2] Shvyryaev P.S. Cybercrime in Russia: a new challenge for society and the state. State Administration. Electronic Bulletin. No. 89, p. 184–196, 2021. DOI: http://dx.doi.org/10.24412/2070-1381-2021-89-184-196 (in Russian).
[3] Vantseva I.O., Zyryanova T.Y., Medvedeva O.O. The impact of the federal law «On the security of the critical information infrastructure of the Russian Federation» on the owners of critical information infrastructures.

Bulletin of the Ural Federal District. Information security. No. 4, p. 71–76, 2018. ISSN 2225-5435. URL: http://info-secur.ru/is_1_2018.pdf (accessed: 01.01.2022) (in Russian).

[4] Deeva T.V. Creation of a unified system of countering cyberattacks: a response to major challenges and threats to the country's tax security. Market economy problems. No. 4, p. 100–112, 2020. ISSN 2500-2325. URL: https://www.elibrary.ru/item.asp?id=44682826 (accessed: 08.01.2022) (in Russian).

[5] Zavorina L.D., Selifanov V.V. Development of an information protection system for a significant object of the critical infrastructure of the Russian Federation. Collection of scientific papers of the Novosibirsk State Technical University. No. 1, p. 123–131, 2018. ISSN 2307-6879. URL: https://www.elibrary.ru/item.asp?id=39157958 (accessed: 08.01.2022) (in Russian).

[6] Gavdan Grigory P., Ivanenko Vitaly G., Salkutsan Aleksey A. Ensuring the safety of significant objects of the KII. Information Technology Security, [S.l.], vol. 26, no. 4, p. 69–82, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.05 (in Russian).

[7] Zyryanova T.Y. Analysis of the requirements of the third category of importance of CII objects in the enterprise infrastructure. Bulletin of the Ural Federal District. Information security. No. 3, p. 69–72, 2019. ISSN 2225-5435. URL: https://www.elibrary.ru/item.asp?id=41151823 (accessed: 08.01.2022) (in Russian).

[8] Kozmins S.I. Interaction of objects of the fuel and energy complex with GosSOPKA. Information resources of Russia. No. 1, p. 2–7, 2020. ISSN 0204-3653. URL: https://www.elibrary.ru/item.asp?id=42512104 (accessed: 08.01.2022) (in Russian).

[9] Kanner Tatyana M. Peculiarities of advanced training of specialists in ensuring the security of significant objects of critical information infrastructure. Information Technology Security, [S.l.], vol. 26, no. 3, p. 22–31, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.3.02 (in Russian).

[10] Kuznetsov S.A., Kulikov I.A., Fominykh A.A. Comparison of CII and CII categorization methods in the Russian Federation and the USA. Actual scientific research in the modern world. No. 6-1, p. 63–68, 2021. ISSN 2524-0986. URL: https://www.elibrary.ru/item.asp?id=46326396 (accessed: 08.01.2022) (in Russian).

[11] Miloslavskaya N.G. Designing Network Security Centers in Information and Telecommunication Networks. M.: Hotline-Telcom. 2020. – 461 p. (in Russian).

[12] Bidou Renaud. Security Operation Center Concepts & Implementation. 2005. URL: http://iv2-technologies.com/~rbidou/SOCConceptAndImplementation.pdf (accessed: 30.12.2021).

[13] Natashova Kristina V. et all. On the issue of categorization of objects of critical information infrastructure of seaports. Information Technology Security, [S.l.], vol. 27, no. 2, p. 35–46, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.2.03 (in Russian).

[14] Miloslavskaya N.G. Information Security Management in SOCs and SICs. Journal of Intelligent & Fussy Systems. Vol. 35, no. 3, p. 2637–2647, 2016. ISBN 1875-8967. URL: https://www.elibrary.ru/item.asp?id=38633644.

[15] Miloslavskaya Natalia G. Information Security Operations Centers. IT Security (Russia), [S.l.], vol. 23, no. 4, p. 38–51, 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/257 (accessed: 09.01. 2022) (in Russian).

[16] Lebedev Pavel. Sberbank Will Protect Itself with the Help of Artificial Intelligence. 2016. URL:https://banks.cnews.ru/news/top/2016-06-10_sberbank_obezopasit_sebya_s_pomoshchyu_iskusstvennogo (accessed: 30.12.2021) (in Russian).

Поступила в редакцию – 05 января 2022 г. Окончательный вариант – 17 февраля 2022 г.
Received – January 05, 2022. The final version – February 17, 2022.

Егор А. Симахин[1], Анатолий П. Дураковский[2], Григорий П. Гавдан[3],
Леонид Н. Кессаринский[4]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: EASimakhin@mephi.ru, https://orcid.org/0000-0003-4019-9694
[2]e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735
[3]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[4]e-mail: LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166

АНАЛИЗ КОМПОНЕНТОВ АРХИТЕКТУРЫ ИНТЕРФЕЙСА DisplayPort, ВЛИЯЮЩИХ НА ПОБОЧНОЕ ЭЛЕКТРОМАГНИТНОЕ ИЗЛУЧЕНИЕ

DOI: http://dx.doi.org/10.26583/bit.2022.1.10

Аннотация. Целью статьи является определение возможных подходов к анализу побочных электромагнитных излучений (ПЭМИ) мониторов с интерфейсом DisplayPort в рамках инструментальных исследований защищенности информации, обрабатываемой средствами вычислительной техники (СВТ). В качестве исследуемого СВТ рассматривается автоматизированное рабочее место с одним монитором и, соответственно, спецификация относительно однопоточного режима передачи видеосигнала. Для достижения цели в статье исследуются компоненты архитектуры интерфейса DisplayPort, характеристики среды распространения сигнала от источника к приемнику и алгоритм формирования транспортных блоков данных. Описывается взаимосвязь количества активных линий передачи данных, тактовой частоты на линию и характеристик пересылаемых данных. Поставлен эксперимент, результаты которого показали, что мощность ПЭМИ зависит от экранирующих мер, применяемых в конструкции кабеля. При проведении исследования компонентов архитектуры интерфейса, влияющих на распределение энергии ПЭМИ в спектре, определено, что помехоустойчивость линий основного канала зависит от настроек конфигурации интерфейса DisplayPort – DPCD. Такая зависимость обуславливает возможность изменения конфигурации (например, скремблирование, шифрование данных и применение частотной модуляции с расширенным спектром) программными средствами и таким образом существенно влиять на качество проведения инструментальных испытаний по оценке защищенности обрабатываемой информации. По результатам исследования предложен порядок анализа необходимой информации для применения подходов и разработан порядок применения инструментальных действий при подготовке к лабораторным исследованиям, что позволит получить более точные значения мощности полезного сигнала при проведении контроля защищенности обрабатываемой информации СВТ с интерфейсом DisplayPort. Дальнейшее исследование будет направлено на апробацию описанных подходов в лабораторных условиях эксплуатации.

Ключевые слова: информационная безопасность, побочное электромагнитное излучение, DisplayPort, безэховая камера, лабораторные исследования.

Для цитирования: СИМАХИН, Егор А. и др. АНАЛИЗ КОМПОНЕНТОВ АРХИТЕКТУРЫ ИНТЕРФЕЙСА DisplayPort, ВЛИЯЮЩИХ НА ПОБОЧНОЕ ЭЛЕКТРОМАГНИТНОЕ ИЗЛУЧЕНИЕ. Безопасность информационных технологий, [S.l.], т. 29, №. 1, p. 108–124, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1410. DOI: http://dx.doi.org/10.26583/bit.2022.1.10.

Благодарности. *Работа выполнена в рамках «Гранта ИБ МТУСИ» Федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации». Грант выдан Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, оператор конкурса грантов Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования Московский технический университет связи и информатики (МТУСИ), № соглашения 40469-28/2021-К.*

Egor A. Simakhin[1], Anatoly P. Durakovskiy[2], Grigory P. Gavdan[3],
Leonid N. Kessarinskiy[4]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[1]e-mail: EASimakhin@mephi.ru, https://orcid.org/0000-0003-4019-9694
[2]e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735
[3]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[4]e-mail: LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166

Analysis of the components of the DisplayPort interface architecture that affect the side electromagnetic radiation

DOI: http://dx.doi.org/10.26583/bit.2022.1.10

Abstract. The present paper aims to determine possible approaches to the analysis of side electromagnetic radiation (EMR) of the monitor video subsystem with the DisplayPort interface within the framework of the investigation of computer processed information (CPI) security. An automated workplace with a single monitor and, accordingly, a specification for a single-threaded video signal transmission mode is considered as the CPI under study. In order to achieve this aim, the components of the DisplayPort interface architecture, the characteristics of the signal propagation medium from the source to the receiver and algorithm for forming transport units have been studied. The correlation between the number of active data transmission lines, the clock frequency per line and the characteristics of the transmitted data are described. The conducted experiment has shown that the power of the EMR depends on the shielding actions used in the cable design. When studying the interface architecture components that affect the EMR energy spectrum, it was found that the interference immunity of the main channel lines depends on the settings of the DisplayPort - DPCD. This dependence makes possible to change the configuration (for example, scrambling, data encryption and the use of frequency modulation with an extended spectrum) by software tools and thus significantly affect the quality of laboratory testing. Based on the results of the present study, a procedure for analyzing the necessary information for the application of approaches is proposed and the procedure for applying instrumental actions in preparation for laboratory studies is developed. This will allow obtaining more accurate values of the power of the useful signal when monitoring the processed information security of the CPI with the DisplayPort interface. Further research will be aimed at laboratory tests of the described approaches under operating conditions.
Keywords: information security, side electromagnetic radiation, DisplayPort, anechoic chamber, laboratory tests.
For citation. SIMAKHIN, Egor A. et al. Analysis of the components of the DisplayPort interface architecture that affect the side electromagnetic radiation. IT Security (Russia), [S.l.], v. 29, n. 1, p. 108–124, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1410. DOI: http://dx.doi.org/10.26583/bit.2022.1.10.

***Acknowledgement**. The work was supported by the "IB MTUCI Grant" of the Federal Project "Information Security" of the national program "Digital Economy of the Russian Federation". The grant was issued by the Ministry of Digital Development, Communications and Mass Communications of the Russian Federation, the operator of the Moscow Technical University of Communications and Informatics (MTUCI), contract №. 40469-28/2021-K.*

Введение

Одним из существенных факторов обеспечения защищенности информации, обрабатываемой средствами вычислительной техники (СВТ), является противодействие утечке защищаемой информации за счет побочных электромагнитных излучений и наводок (ПЭМИН). Исследования в данном направлении показывают возможность обнаружения уязвимых интерфейсов передачи данных СВТ. В [1], например, автор исследовал побочные электромагнитные излучения (ПЭМИ) от четырех мониторов с жидкокристаллическим дисплеем, оценил зависимость формата и параметров синхронизации. В [2] исследованы принципы утечки информации с использованием дифференциальных сигнальных кабелей,

таких как кабель мультимедийного интерфейса высокой четкости (HDMI), кабель цифрового визуального интерфейса (DVI) и кабель низковольтной дифференциальной сигнализации (LVDS). В этой же работе показано, что побочные электромагнитные излучения (ПЭМИ) от дифференциальных сигнальных кабелей имеют не только амплитудную модуляцию, но и частотную модуляцию, что существенно расширяет возможности злоумышленникам для перехвата и последующего восстановления полезной информации. В [3–5] приведены результаты исследований ПЭМИ от HDMI, USB-накопителя, USB-разъема и контроллера. Результаты исследований перехвата и последующего восстановления полезной информации из исходящего видеосигнала приведены в [6–10]. Наряду с этим, проводятся исследования по анализу подходов к обеспечению требуемого уровня защищенности СВТ [11] и разработке программно-аппаратных комплексов для решения задачи тестирования систем защиты информации [12–13].

С возросшим объемом обрабатываемой информации обширное распространение получили мониторы с высокоскоростными интерфейсами передачи данных, например, HDMI и DisplayPort. Исследования побочных электромагнитных излучений (ПЭМИ) мониторов с подобными интерфейсами вызывают особый интерес со стороны специалистов по технической защите информации, в частности работы с экспериментальным обоснованием.

Исследования такого рода регламентируются методическими рекомендациями, в целом определяющими порядок действий при проведении контроля защищенности СВТ. Для разработки подобных рекомендаций требуется проведение анализа характеристик рассматриваемого интерфейса, его спецификации, описание подхода к обнаружению информативных частот и инструментальное подтверждение в лабораторных или реальных условиях эксплуатации. В настоящее время решение описываемой задачи для высокоскоростных интерфейсов передачи данных частично определено, в частности, например, для интерфейса HDMI [14] и отсутствует для интерфейса DisplayPort, вследствие чего не представляется возможным сформировать методические рекомендации при отсутствии четко определенных подходов к анализу ПЭМИ мониторов с интерфейсом DisplayPort.

Для решения данной проблемы требуется провести анализ технологии DisplayPort и на основании полученных сведений сформировать возможные подходы к анализу ПЭМИ мониторов с интерфейсом DisplayPort в рамках лабораторных исследований защищенности СВТ, что и является целью статьи.

1. Анализ технологии DisplayPort

Впервые спецификация интерфейса DisplayPort была принята Ассоциацией стандартизации видеоэлектроники (VESA) еще в 2006 г.[1]. Данный стандарт должен был удовлетворить межотраслевые потребности и решить технические задачи по их обеспечению. Одной из таких задач является применение встроенных в архитектуру интерфейса функций для снижения восприимчивости к электромагнитным помехам и уменьшения количества линий передачи. Иными словами, характеристики разработанного интерфейса должны соответствовать требованиям межгосударственных стандартов, относящихся к деятельности подкомитета CIS/B Специального международного комитета по радиопомехам (CISPR): «Помехи, относящиеся к промышленному, научному и медицинскому радиочастотному оборудованию, к другому (тяжелому) промышленному

[1]VESA DisplayPort Standard Version 1, Revision 2, 2010. URL: https://glenwing.github.io/docs/DP-1.2.pdf. (дата обращения: 11.02.2022).

оборудованию, к воздушным линиям электропередач, к высоковольтному оборудованию и к электрической тяге».

В настоящее время утверждено несколько версий данного стандарта, начиная от версии 1.0 до актуальной версии – 2.0, принятой в 2019 г. В связи с преимуществом технологии DisplayPort, VESA ограничила возможность ознакомления с интеллектуальной собственностью и в открытом доступе представлены спецификации интерфейса только до версии стандарта 1.2 включительно, которая рассматривается в статье.

Для формирования подходов к анализу ПЭМИ монитора с интерфейсом DisplayPort, необходимо, исходя из спецификации, определить характеристики технологии, влияющие на утечку информации по рассматриваемому техническому каналу. Для решения данной задачи следует проанализировать принципы его работы, архитектуру интерфейса, среду распространения сигнала от источника к приемнику и алгоритм формирования данных для их передачи.

1.1 Доступные режимы работы

До проведения инструментальных испытаний защищенности обрабатываемой информации для каждого СВТ определяют требуемые условия его эксплуатации для исполнения служебных обязанностей сотрудниками. Стандарт описывает передачу данных в двух режимах: Single Stream Transport (SST) и Multi-Stream Transport (MST). Режим MST объединяет несколько видеосигналов в один поток и позволяет транслировать независимые изображения с одного настольного компьютера или ноутбука, формировать последовательное подключение нескольких мониторов с помощью одного соединения – «Гирляндная цепь», расширять экран монитора и дублировать изображение рабочего стола на вспомогательные или дополнительные мониторы. В режиме SST видеосигнал передается по умолчанию в виде одного потока на один монитор. Исходя из наиболее распространенного вида СВТ в организации – это автоматизированное рабочее место с одним монитором, для которого в данной статье рассматривается спецификация относительно однопоточного режима передачи.

В соответствии с рассматриваемой спецификацией для корректной передачи потока данных интерфейс DisplayPort имеет основной канал (Main Link), вспомогательный канал (Auxiliary channel – AUX CH) и линию «горячего подключения» (Hot Plug Detect – HPD). Основной канал представляет собой однонаправленный канал с высокой пропускной способностью и малой задержкой, используемый для изохронной передачи данных. Вспомогательный канал представляет собой полудуплексный двунаправленный канал, используемый для управления каналом связи. Линия HPD обслуживает запросы на прерывание работы (сопряжение, наличие ошибок, изменения в режиме работы) приемным устройством. Схематично исследуемые каналы интерфейса представлены на рис. 1.

Вследствие изохронности, передача данных от источника к приемнику осуществляется с постоянной скоростью. Для обеспечения этого основной канал поддерживает три варианта количества линий – 1, 2 и 4, три скорости передачи на полосу – 1,62 Гбит/с, 2,7 Гбит/с и 5,4 Гбит/с, что определяет три режима работы интерфейса – RBR, HBR, HBR2.

Соответствие скорости передачи данных, пропускной способности и количества задействованных линий режимам работы представлено в табл. 1.

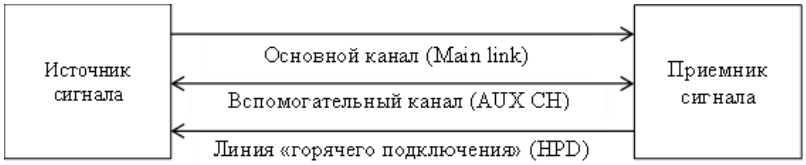


Рис. 1. Каналы интерфейса DisplayPort
Fig. 1. DisplayPort interface channels

Таблица 1. Режимы работы интерфейса DisplayPort

Режим работы	Количество линий	Пропускная способность на линию		
		1,62 Гбит/с	2,7 Гбит/с	5,4 Гбит/с
RBR	1	162 Мбайт/с	270 Мбайт/с	540 Мбайт/с
HBR	2	324 Мбайт/с	540 Мбайт/с	1080 Мбайт/с
HBR2	4	648 Мбайт/с	1080 Мбайт/с	2160 Мбайт/с

Скорость передачи данных на линию и, соответственно, их количество определяется возможностями источника и приемника, качеством кабеля. Для выбора скорости передачи данных приемное устройство записывает свои возможности в поля метаданных для устройств отображения – Extended Display Identification Data (EDID) и в поля настроек интерфейса – DisplayPort Configuration Data (DPCD), а источник, после передачи сигнала обнаружения HPD, проверяет предоставленные данные. При повреждении данных EDID, источник выбирает один из набора конфигураций резервных форматов видео. Если ни один из резервных форматов не является приемлемым, источник выбирает конфигурацию отказоустойчивого режима: 640*480, 60 Гц в соответствии со стандартом VESA DMT[2]. При успешном считывании конфигурации приемника следует этап настройки и тестирования соединения, за что отвечает режим Link Training.

Согласно стандарту, для корректной передачи данных источник и приемник могут поддерживать минимальное количество линий. Вследствие этого, устройства, поддерживающие две линии передачи данных, должны поддерживать режимы работы RBR и HBR, в то время как устройства, поддерживающие четыре линии передачи данных, должны поддерживать режимы работы RBR, HBR и HBR2. При успешном результате тестирования источник и приемник согласовывают оптимальное количество линий, скорость передачи данных и, как следствие, тактовую частоту передачи на линию. Для интерфейса DisplayPort 1.2 определено несколько значений тактовых частот передачи: 162 МГц, 270 МГц и 540 МГц. Зависимость тактовой частоты передачи от пропускной способности на линию представлена в табл. 2.

Таблица 2. Тактовая частота основного канала

Пропускная способность на линию	Тактовая частота передачи «symbol»
1,62 Гбит/с	162 МГц
2,7 Гбит/с	270 МГц
5,4 Гбит/с	540 МГц

В качестве единицы передачи информации в стандарте принято обозначение «symbol». За «symbol» принимается 8 бит данных, кодируемых до момента их передачи в 10 бит в соответствии с пунктом 11 стандарта ANSI X3.230-1994, чем и объясняется представленная зависимость.

[2]VESA and Industry Standards and Guidelines for Computer Display Monitor Timing (DMT) Version 1.0, Rev. 13, 2013. URL: https://glenwing.github.io/docs/VESA-DMT-1.13.pdf. (дата обращения: 11.02.2022).

В связи с возможностью выбора количества линий передачи данных основного канала, различных форматов видео (720x480 чересстрочное, 60 Гц; 1280x720 прогрессивное, 60 Гц; и др.) и поддержки минимального количества линий стандарт предусматривает наличие функции изменения (увеличение/уменьшение) количества активных линий. Алгоритмы работы функции изменения количества активных линий представлен на рис. 2 и 3. Принцип работы функции изменения:

1) Увеличение количества активных линий (для режимов с 1 линией и 2 линиями).

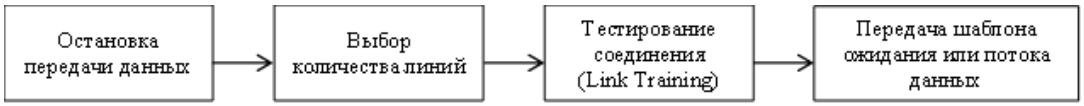


Рис. 2. Алгоритм увеличения количества активных линий
Fig. 2. Algorithm for increasing the number of active lines

Шаблоном ожидания, согласно стандарту, называется последовательность данных, пересылаемая по активной линии, в отсутствие потоковых данных. Под активной линией передачи данных подразумевается линия основного канала, используемая для передачи данных.

2) Уменьшение количества активных линий (для режимов с 2 и 4 линиями)

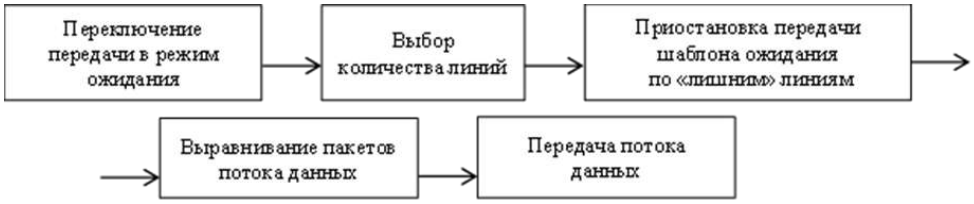


Рис. 3. Алгоритм уменьшения количества активных линий
Fig. 3. Algorithm for reducing the number of active lines

Стоит отметить, что при изменении количества активных линий не изменяются значения битовой глубины пикселя, битовой глубины компонента и формата колориметрии RGB, YC_bC_r в том числе с различной цветовой субдискретизацией 4:4:4/4:2:2.

Вследствие того, что количество активных линий влияет на изменение тактовой частоты передачи данных СВТ с интерфейсом DisplayPort, то на этапе подготовки к лабораторным исследованиям следует:

1) провести анализ EDID и уточнить характеристики используемого монитора;

2) выбрать режим(ы) работы, для исключения не контролируемой смены количества активных линий;

3) оценить количество активных линий при использовании выбранных режимов работы;

4) определить тактовую частоту на линию для каждого выбранного режима работы.

Определив основные характеристики режимов работы СВТ с интерфейсом DisplayPort, следует проанализировать его архитектуру и определить компоненты, влияющие на проведение лабораторных исследований по техническому каналу ПЭМИН.

1.2 Архитектура интерфейса

Архитектура интерфейса DisplayPort содержит два основных уровня: канальный и физический. Канальный уровень обеспечивает требуемые свойства изохронной передачи данных, основанной на архитектуре микропакетов, управление соединением и устройствами по каналу AUX CH и тактирование приемника сигнала. Физический уровень определяет

физические свойства соединения между источником и приемником, электрические характеристики интерфейса и процедуры подготовки данных к передаче. Взаимодействие источника и приемника обусловлено физической средой распространения сигнала. Общий принцип архитектуры интерфейса DisplayPort приведен на рис. 4.

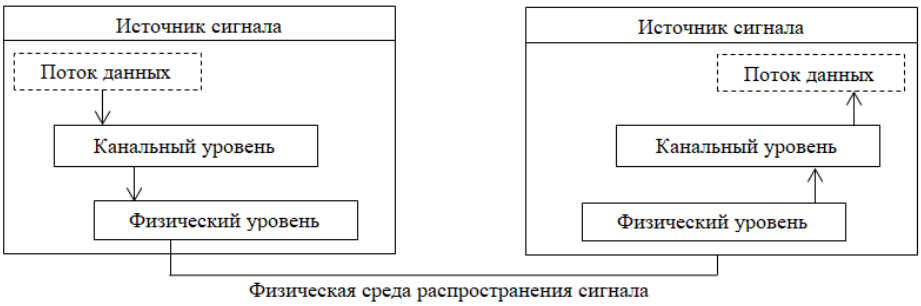


Рис. 4. Общий принцип архитектуры интерфейса DisplayPort
Fig. 4. The general principle of the DisplayPort interface architecture

В целях анализа компонентов архитектуры интерфейса, с точки зрения влияния на проведение лабораторных исследований по техническому каналу ПЭМИН, необходимо сформировать исследовательский стенд, который позволит экспериментально оценить работу интерфейса DisplayPort и его энергетический спектр.

1.2.1 Описание исследовательского стенда

При проведении инструментального контроля защищенности СВТ, связанного с определением максимального расстояния, на котором возможно осуществить восстановление информации за счет анализа характеристик ПЭМИ, прежде всего, оценивают критические условия эксплуатации. Как правило, критические условия определяются минимальным уровнем мощности электромагнитного шума или помех и максимальным уровнем мощности сигнала в окружающем пространстве от исследуемого интерфейса. Минимальный уровень мощности электромагнитного шума достигается особыми условиями проведения испытаний, например выбором времени их проведения, или при использовании альтернативной измерительной площадки (АИП).

В ходе эксперимента, связанного с анализом ПЭМИ интерфейса DisplayPort, в качестве АИП использовалась безэховая экранированная камера со следующими характеристиками:

1) в соответствии с ГОСТ 30373-95 имеет I класс экранирования в диапазоне от 10 кГц до 40 ГГц;

2) соответствует требованиям ГОСТ 53120-99 в диапазоне частот от 30 МГц до 1 ГГц;

3) размеры в единицах метров (длина, ширина, высота): 10,29*5,85*4,16.

В качестве исследуемого объекта использовалось СВТ с интерфейсом DisplayPort со следующими составляющими:

1) монитор AOC 2475W1 с характеристиками, полученными с помощью программного обеспечения для создания и редактирования файлов Extended Display Identification Data– AW EDID Editor, рис. 5.

2) операционная система – Windows 10;

3) материнская плата – Asus Prime B250M-C;

4) версия BIOS – 1050 PC 14.34;

5) видеоадаптер – Intel Skylake-S GT2.

Исследуемое СВТ размещается на диэлектрическом поворотном столе на высоте 80 см от пола, интерфейсный кабель DisplayPort располагается без перекручивания и выпрямлен по всей своей длине. Для исключения возможного появления помех в АИП отсутствуют иные СВТ, что повышает точность результатов эксперимента. Пример расположения монитора представлен на рис. 6.

Рис. 5. Характеристики монитора
Fig. .5 Characteristics of the monitor

Рис. 6. Расположение монитора
Fig. 6. Location of the monitor

Оценивая характеристики монитора, можно заметить, что пиксельная частота численно равна 148,5 МГц и не соответствует ни одному из приведенных выше значений. Связано это с тем, что в архитектуре интерфейса DisplayPort нет отдельного тактового канала и, поэтому для корректного приема видеосигнала используется механизм восстановления пиксельной частоты, а также количество бит, содержащих информацию об одном пикселе больше 8 бит. В соответствии со спецификацией определяется количество бит на пиксель в зависимости от формата колориметрии:

1) для формата RGB:18 бит, 24 бит, 30 бит и 36 бит на пиксель;
2) для формата YC_bC_r (4:2:2): 16 бит, 20 бит, 24 бит и 32 бит на пиксель;
3) для формата YC_bC_r (4:4:4): 24 бит, 30 бит, 36 бит и 48 бит на пиксель.

Количество бит на пиксель для отдельного монитора можно посмотреть по следующему пути реестра операционной системы Windows: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{ID}\{номер порта – 0000} и ключу DefaultSettings.BitsPerPel.

В качестве измерительного приемника использовался анализатор спектра и сигналов Rohde Schwarz FSW 13 с диапазоном частот от 2 Гц до 13,6 ГГц. Для поиска информативных частот интерфейса DisplayPort использовались дипольная антенна АИ5-0 для диапазона от 9 кГц до 2 ГГц, АШН-5 и АШН-6 для диапазона от 2 ГГц до 13,6 ГГц. Все представленные в работе эксперименты и графики получены на представленном оборудовании и АИП.

1.2.2 Физическая среда распространения сигнала

Средой распространения сигнала между источником и приемником является интерфейсный кабель. Согласно спецификации интерфейса DisplayPort 1.2 конструкция кабеля должна быть выполнена таким образом, чтобы его параметры экранирования и устойчивости к электромагнитным помехам соответствовали требованиям межгосударственных стандартов, относящихся к деятельности подкомитета CIS/B CISPR с запасом не менее 6 дБ.

Для оценки влияния принятых мер экранирования на мощность ПЭМИ поставлен следующий эксперимент. Для его проведения взято 2 одинаковых кабеля DisplayPort длиной 5 метров в штатной конфигурации и без слоя экранирующих материалов. В ходе эксперимента были обнаружены спектральные компоненты монитора с интерфейсом

DisplayPort в частотном диапазоне до 2,5 ГГц. Результаты эксперимента представлены на рис. 7.

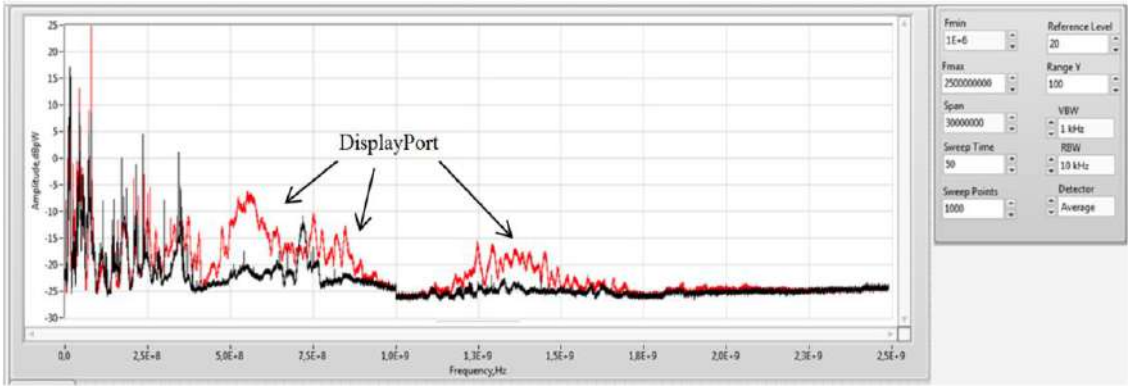


Рис. 7. Результаты эксперимента
Fig. 7. The experiment results

По полученным результатам видно, что принятые меры к экранированию кабеля способствуют уменьшению мощности ПЭМИ, а соответственно их нарушение приводит к критичным условиям эксплуатации. Отсутствие экранирования не влияет на передаваемый сигнал в лабораторных условиях.

Несмотря на результаты эксперимента, деструктивное исследование приводит к нарушению целостности кабеля, отклонению от штатной (заводской) конфигурации интерфейса и снижению уровня помехозащищенности каналов передачи данных, что недопустимо при реальных условиях эксплуатации.

Тем не менее, при подготовке к лабораторным испытаниям специалистам следует убедиться, что кабель не имеет физических повреждений и экранирующий слой не нарушен.

1.2.2.1 Модуляция сигнала

Анализируя график огибающей спектра интерфейса DisplayPort, представленный на рис. 7, можно заметить, что в отличие от интерфейса HDMI спектр сигнала «размыт» по частотам. В соответствии со стандартом для достижения такого эффекта при преобразовании сигнала используется частотная модуляция с расширенным спектром (SSFM). Данный вид частотной модуляции применяется для уменьшения уровня электромагнитных помех при передаче сигнала и эффективно снижает пиковую амплитуду на несущей частоте и ее гармонических частотах [15]. Частота модуляции, применяемая в интерфейсе DisplayPort, определена в диапазоне от 30 кГц до 33 кГц.

Для того чтобы оценить мощность сигнала с достаточной полнотой, необходимо измерить его фильтром равным полосе сигнала, при этом мощности «размытого» и «не размытого» сигналов окажутся одинаковыми. Тем не менее, оборудование, которое позволяет выполнить такую работу, имеет достаточно высокую цену или вовсе недоступно многим лабораториям по причинам ограничения экспортного контроля. Несмотря на это, в конфигурации DPCD возможно отключить применяемое преобразование. Отключение модуляционного преобразования позволит уже разработанными автоматизированными методами обнаружить спектральные компоненты интерфейса DisplayPort и соответственно провести измерение мощности сигнала.

1.2.3 Физический уровень

Физический уровень обеспечивает подготовку к передаче данных и тестирует соединение на наличие ошибок. Функциональная схема физического уровня приведена на рис. 8.

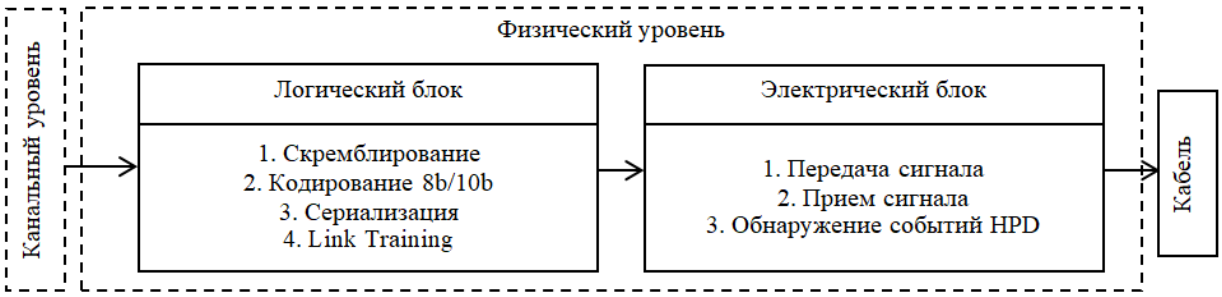


Рис. 8. Физический уровень интерфейса DisplayPort
Fig. 8. Physical layer of the DisplayPort interface

Исходя из функциональной схемы, поток данных поступает на логический блок физического уровня после выполнения функций канального уровня. Первой операцией основного канала в логическом блоке является скремблирование. В этот же момент на вспомогательном канале происходит инициализация соединения в режиме Link Training, в случае, если источник и приемник не синхронизированы. Канал HPD ожидает сигнала об изменении статуса соединения с приемником. Второй операцией основного канала является кодирование в соответствии со стандартом ANSI X3.230-1994. Далее кодированные данные проходят сериализацию.

В рамках инструментальных исследований осуществлять воздействие (отключение) на принимаемые производителем меры по обеспечению помехоустойчивости возможно только при условии отсутствия последующего нарушения работоспособности интерфейса и, как следствие, требований к имитации реальной эксплуатации СВТ. Изменение же принятых в стандарте функции кодирования 8b/10b и сериализации, определяющих порядок приема/передачи данных, может привести к ошибкам при обработке принимаемых данных и их частичной утрате. С этой точки зрения, анализ данных операций является не актуальным.

Тем не менее, с точки зрения формирования тестовой последовательности со скважностью передаваемого сигнала равной 2, кодирование 8b/10b определяет базовое требование: 8 бит/10 бит нулей и 8 бит/10 бит единиц. Порядок следования выполняемых операций относительно каналов передачи представлен на рис. 9.

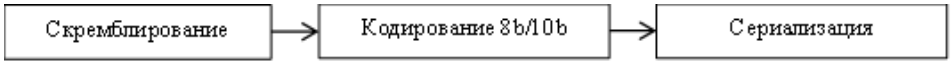


Рис. 9. Порядок выполнения операций на физическом уровне
Fig. 9. The procedure for performing operations at the physical level

Электрический блок осуществляет прием и передачу данных, выполняет функцию обнаружения событий HPD. Осуществление воздействий на электрический блок может привести к нарушению процесса передачи данных, что противоречит штатной работе рассматриваемого интерфейса. Таким образом, анализ функций электрического блока с точки зрения влияния на ПЭМИ является не актуальным. Далее рассмотрим подробнее функции скремблирования и режим Link Training.

1.2.3.1 Функция скремблирования

В соответствии со спецификацией интерфейса DisplayPort версии 1.2 скремблер реализован не на аппаратном уровне, а его применение приводит к уменьшению уровня мощности ПЭМИ информативного сигнала примерно на 7 дБ. Эталонная реализация скремблера на языке С представлена в приложении «Е» стандарта и включает в себя методы надежного обнаружения управляющего бита SR, приостанавливающего работу скремблера. Следовательно, можно предположить, что программными средствами можно управлять работой скремблера при передаче данных по интерфейсу DisplayPort. Например, осуществить изменение настроек DPCD, отвечающих за отключение скремблера, возможно, используя управляющие команды инструкций технологических компаний, например, таких как Intel[3] и Altera[4].

Дополнительно, для решения задачи отключения скремблера может быть разработан программно-аппаратный комплекс (ПАК) на базе программируемой логической интегральной схемы (ПЛИС) с двумя разъемами DisplayPort – Male и Female. Функционально ПЛИС должно повторять приемно-передающее устройство по стандарту DisplayPort с ограниченным функционалом, позволяющим выполнить обратное преобразование скремблера на ПЛИС №1 и скремблирование на ПЛИС №2. Дополнительно ПЛИС должны поддерживать реализацию функций каналов AUX CH и HPD, а также функционал, выполняемый после этапа скремблирования. Предполагаемый принцип внедрения при лабораторных исследованиях показан на рис. 10, где разъем DisplayPort Male – DPM, разъем DisplayPort Female – DPF.

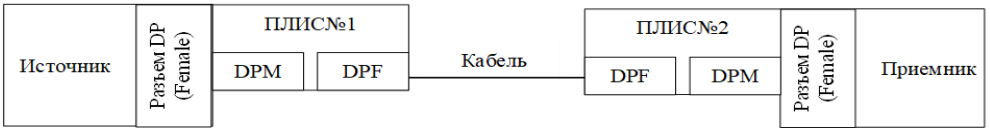


Рис. 10. Предполагаемый принцип использования ПЛИС
Fig. 10. The proposed principle of using a programmable logic integrated circuit

Основным недостатком использования решения с ПЛИС является наличие дополнительных электромагнитных помех. К тому же, для использования такого подхода требуется проведение тестирования функций ПЛИС, ее программного обеспечения в момент подготовки к лабораторным испытаниям, что увеличивает трудозатраты.

1.2.3.2 Режим Link Training

Настройка и тестирование соединения происходит с помощью определения параметров DPCD и их изменения в соответствии с возможностями приемника и источника. Благодаря процессу определения возможностей приемника и настройке канала связи источник и приемник DisplayPort избегают ошибок при передаче данных, согласовывают оптимальное количество линий и скорость передачи данных на линию для данного соединения.

[3]DisplayPort Intel® FPGA IP User Guide, 2021. URL: https://www.intel.com/content/www/programmable/us/en/literature/ug/ug_displayport.pdf (дата обращения: 21.02.2022).
[4]DisplayPort IP Core User Guide, 2016. URL: https://www.intel.com/content/dam/altera-www/global/ja_JP/pdfs/literature/ug/ug_displayport.pdf (дата обращения: 21.02.2022).

Особенность режима Link Training в том, что при его работе не активен скремблер. С учетом того, что логика режима реализована в драйвере DisplayPort, то при изменении программного кода драйвера данный режим можно использовать для максимальной нагрузки линий по основному каналу. За основу кода с изменениями можно использовать репозиторий с открытым исходным кодом драйвера для режима Link Training интерфейса DisplayPort версии 1.2[5], распространяющегося под публичной лицензией GNU. Недостатком данного подхода является то, что для его реализации требуется дополнительное функциональное тестирование изменений драйвера и оценка их влияния на передачу данных в штатном режиме.

1.2.4 Канальный уровень

Канальный уровень определяет формирование блоков данных, их порядок передачи и обеспечивает защищенность передаваемой информации посредством технологии High-bandwidth Digital Content Protection (HDCP) с поправками указанными в стандарте. В целях формирования тестовой последовательности, следующей правилу «8 бит/10 бит нули и 8 бит/10 бит единицы», необходимо рассмотреть функционал канального уровня, рис. 11.

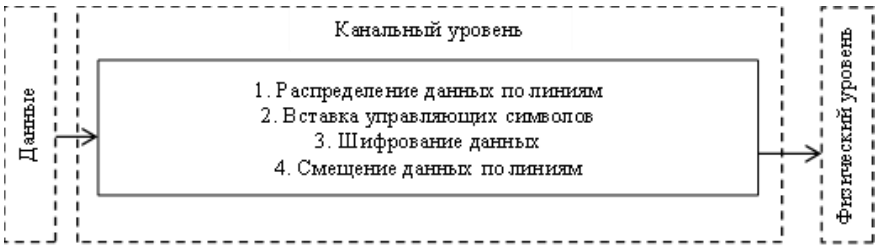


Рис.11. Канальный уровень интерфейса DisplayPort
Fig.11. Channel level of the DisplayPort interface

Исходя из функциональной схемы, поток данных поступает на канальный уровень, преобразуется в удобный для передачи и восстановления исходного изображения вид и передается на физический уровень. Первой операцией канального уровня является распределение данных по линиям. В случае одной линии все данные пересылаются только по ней. В случае двух линий, данные распределяются по законам: $2n$ для линии «0» и $2n+1$ для линии «1», где n – номер линии. Для четырех линий по законам: $4n$ для линии «0», $4n+1$ для линии «1», $4n+2$ для линии «2» и $4n+3$ для линии «3».

В целях кадрирования, разделения на транспортные блоки и уведомления преемника о типе пересылаемых данных в соответствии со стандартом применяется вставка управляющих символов.

Вставка управляющих символов происходит следующим образом:

1) Первый цикл на каждой линии содержит запись управляющего символа BE для указания места начала данных. Далее следует набор пересылаемых данных.

2) Применение операции заполнения нулевыми данными на каждой активной линии до размера транспортного блока. Транспортный блок содержит от 32 до 64 символов на линию и может менять размер в зависимости от передаваемого формата видео.

3) После последнего цикла добавления данных на всех линиях вставляется управляющий символ BS, показывающий место конца блока передачи.

[5]DisplayPort-link-training, 2016. URL: https://github.com/ankishore/DisplayPort-link-training. (дата обращения: 21.02.2022).

4) Уведомление о пересылке аудио, видео и их характеристиках реализовано с помощью управляющих символов Maud7:0, Mvid7:0 и VB-ID соответственно. При отсутствии передачи аудио или видео символы Maud7:0, Mvid7:0 сбрасываются в состояние 00h.

5) Далее на каждой линии следует поле свободных бит, либо заполненных фиктивными данными, либо аудиоданными, обрамленными управляющими символами FS и FE.

6) Транспортный блок окончен.

Для обеспечения защиты пересылаемых данных в стандарте предусмотрена операция шифрования на базе технологии HDCP версии 1.3. Для формирования тестовой последовательности, необходимо знать значение векторов инициализации приемника и источника сигнала, а также 64-битное число. Как правило, такие данные недоступны, из-за чего возникают трудности при формировании тестовой последовательности. Тем не менее, преодолеть это возможно с помощью пакета AMD Radeon Software или устройств HDCP-stipper.

В целях помехоустойчивости канала передачи применяется операция смещения данных между линиями. Первая линия не смещается, а каждая последующая относительно предыдущей линии смещается на два цикла заполнения символами. В случае появления внешних помех такой принцип позволяет исключить потерю символов одного типа для всех линий, например управляющих символов.

Результат базовых преобразований канального уровня, исключая шифрование, представлен на рис. 12, где серым цветом отмечены области фиктивных данных, У1 (BE) и У2 (BS, VB-ID, Mvid7:0, Maud7:0, FS, FE) обозначены области управляющих символов, П* и «.» –области данных и «0» – область заполненная нулями.

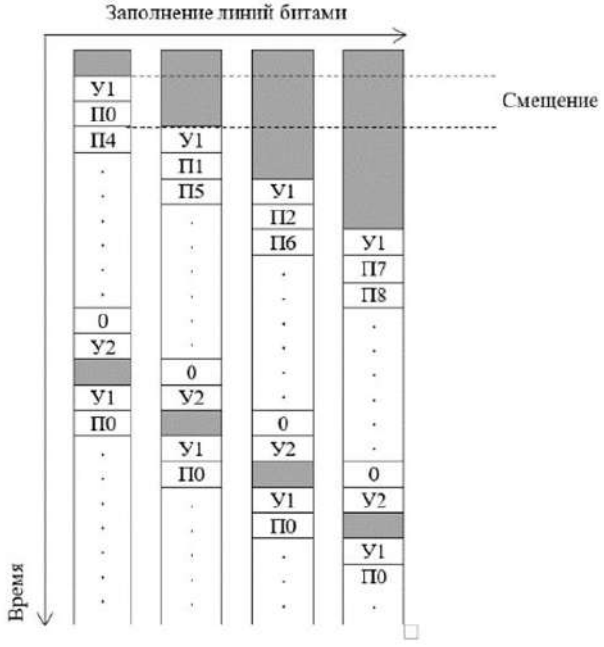


Рис.12 Состояние перед передачей на физический уровень
Fig.12 The state before transmission to the physical layer

Таким образом, функцией влияющей на формирование тестовой последовательности является только операция шифрования на базе технологии HDCP версии 1.3. Результат же

работы функций распределения данных по линиям, вставки управляющих символов и смещения символов стоит учитывать при оценке влияния тестовой последовательности на мощность излучения.

2. Возможные подходы к анализу ПЭМИ

Из вышеприведенного следует, что подходы к анализу ПЭМИ интерфейса DisplayPort при условии создания критических условий касаются:

1) подготовительного этапа к лабораторным испытаниям;
2) отключения внутреннего функционала, не влияющего на работу интерфейса;
3) использования сведений для создания тестовой последовательности.

В табл. 3 представлены основное содержание подходов к анализу, результат их использования и недостатки по отношению к принятому порядку проведения лабораторных испытаний. Основным недостатком является функциональное тестирование результатов применяемых подходов, что автоматически приводит к увеличению трудозатрат проводимых исследований. Дополнительно, для обеспечения штатной работы СВТ после проведения лабораторных испытаний необходимо выполнить повторное включение всех отключенных функций, влияющих на ПЭМИ интерфейса DisplayPort, что также, хоть и незначительно, увеличивает трудозатраты.

Таблица 3. Подходы к анализу

Подход к анализу	Содержание подхода	Результат	Недостатки
Подготовительный этапа к испытаниям	Анализ EDID	Уточнение характеристик монитора	Увеличение трудозатрат
	Выбор режима(ов) работы монитора	Исключение не контролируемой смены количества активных линий	
	Определение количества активных линий	Определение тактовой частоты передачи на линию	
Отключение внутреннего функционала	Передача данных при работе режима Link Training	Отключение скремблера	• Функциональное тестирование и оценка влияния на передачу данных в штатном режиме изменений драйвера • Повторный запуск • Увеличение трудозатрат
	Разработка ПАК на базе ПЛИС		• Наличие дополнительных электромагнитных помех • Тестирование функций ПЛИС и ее программного обеспечения • Повторный запуск • Увеличение трудозатрат
	Использование AMD Radeon Software, HDCP-stipper	Отключение HDCP	• Повторный запуск • Увеличение трудозатрат
	Анализ преобразования модуляции SSFM	Отключение SSFM	• Повторный запуск • Увеличение трудозатрат
Использование сведений для создания тестовой последовательности	Анализ порядка передачи символов	Формирование тестовой последовательности	• Тестирование влияния последовательности на работу интерфейса • Увеличение трудозатрат
	Оценка влияния тестовой последовательности на мощность излучения		

В соответствии с табл. 3 можно определить порядок анализа необходимой информации для применения подходов и последовательность применения инструментальных действий при подготовке к лабораторным исследованиям, что показано на рис. 13 и 14 соответственно.

Рис. 13. Порядок анализа необходимой информации
Fig. 13. The procedure for analyzing the necessary information

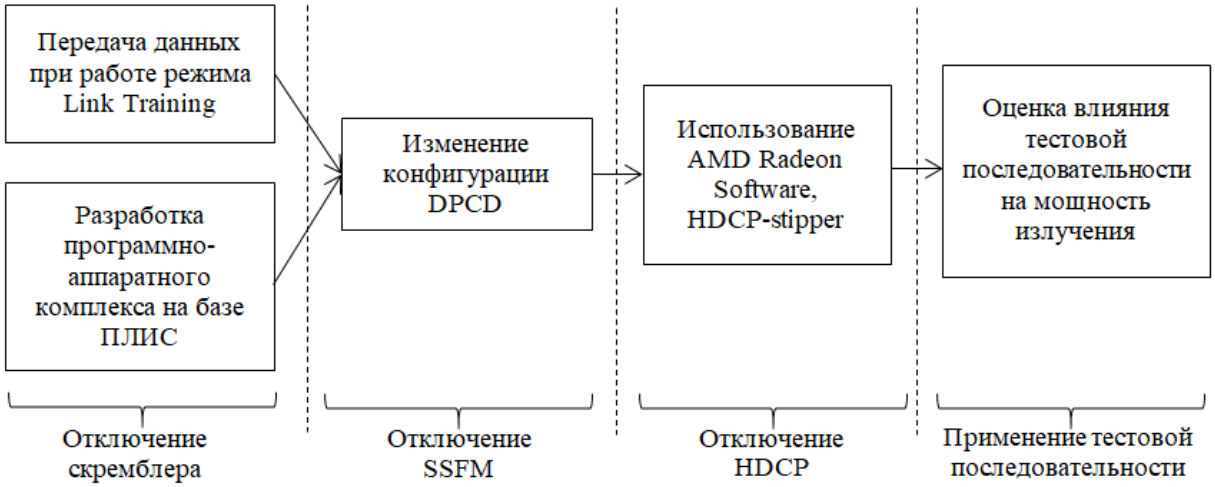


Рис. 14. Последовательность применения инструментальных действий
Fig. 14. The sequence of application of instrumental actions

Заключение

В данной статье проанализирована архитектура интерфейса DisplayPort 1.2 и описаны подходы к анализу излучения монитора с интерфейсом DisplayPort в рамках лабораторных исследований по техническому каналу ПЭМИН. На основании спецификации, определены характеристики интерфейса, влияющие на мощность побочного электромагнитного излучения: режим работы монитора, экранирующие материалы, скремблирование, шифрование данных и SSFM. По результатам исследования предложен порядок анализа необходимой информации для применения подходов и разработан порядок применения инструментальных действий при подготовке к лабораторным исследованиям, что позволит получить более точные значения мощности полезного сигнала при проведении контроля защищенности обрабатываемой информации СВТ с интерфейсом DisplayPort. Дальнейшее исследование будет направлено на апробацию описанных подходов при лабораторных исследованиях монитора с интерфейсом DisplayPort.

СПИСОК ЛИТЕРАТУРЫ:

1. M.G. Kuhn. Compromising emanations of LCD TV sets, in IEEE Transaction on electromagnetic compatibility. Vol. 55, no. 3, 2013, p. 564–570. DOI: http://dx.doi.org/10.1109/TEMC.2013.2252353.
2. P. De Meulemeester, B. Sheers, G. A. E. Vandenbosch. Differential signaling compromises video information security through AM and FM leakage emissions, in IEEE Transactions on Electromagnetic Compatibility. Vol. 62, no. 6, p. 2376–2385, 2020. DOI: http://dx.doi.org/10.1109/TEMC.2020.3000830.
3. Ivanov A.V., Reva I.L., Ushakov A.E. Features of identification and the analysis of collateral electromagnetic radiations from USB flash drives, Proceedings of 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE). 2016, p. 156–158. DOI: http://dx.doi.org/10.1109/APEIE.2016.7806436.
4. Durakovskiy A.P., Kessarinskiy L.N., Simakhin E.A. Detection of compromising radiation from modern data transfer interfaces using the example of high definition multimedia interface, IOP Conference Series: Materials Science and Engineering. 1069(1), 7, ISSN 1757-8981, 2021. DOI: http://dx.doi.org/10.1088/1757-899X/1069/1/012026.
5. R. Birukawa, D. Nagata, Y. -i. Hayashi, T. Mizuki and H. Sone. The Source Estimation of Electromagnetic Information Leakage from Information Devices, 2020 XXXIIIrd General Assembly and Scientific Symposium of the International Union of Radio Science. 2020, p. 1–4. DOI: http://dx.doi.org/10.23919/URSIGASS49373.2020.9231979.
6. T. Song, Y. Jeong, J. Yook. Modeling of Leaked Digital Video Signal and Information Recovery Rate as a Function of SNR, in IEEE Transactions on Electromagnetic Compatibility. Vol. 57, no. 2, 2015, p. 164–172. DOI: http://dx.doi.org/10.1109/TEMC.2014.2372039.
7. Sokolov R.I., Abdullin R.R., Dolmatov D.A. Development of Synchronization System for Signal Reception and Recovery from USB-Keyboard, Proceedings of 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). 2016, p. 1–4. DOI: http://dx.doi.org/10.1109/ICIEAM.2016.7911553.
8. Degang Sun, Di Wei, Ning Zhang, Z Lv, Xi Yin. Network transmission of hidden data using smartphones based on compromising emanations, Proceedings of 7th Asia Pacific International Symposium on Electromagnetic Compatibility (APEMC). 2016, p. 190–193. DOI: http://dx.doi.org/10.1109/APEMC.2016.7523005.
9. P. De Meulemeester, B. Scheers, G. A. E. Vandenbosch. A Quantitative Approach to Eavesdrop Video Display Systems Exploiting Multiple Electromagnetic Leakage Channels, in IEEE Transactions on Electromagnetic Compatibility. Vol. 62, no. 3, p. 663–672, 2020. DOI: http://dx.doi.org/10.1109/TEMC.2019.2923026.
10. P. De Meulemeester, B. Scheers, G. A. E. Vandenbosch. Reconstructing Video Images in Color Exploiting Compromising Video Emanations, Proceedings of 2020 International Symposium on Electromagnetic Compatibility - EMC EUROPE. 2020, p. 1–6. DOI: http://dx.doi.org/10.1109/EMCEUROPE48519.2020.9245775.
11. Голяков Александр А.; Дураковский Анатолий П.; Симахин Егор А. Применение генератора замещения для определения реального затухания информативных сигналов побочных электромагнитных излучений. Безопасность информационных технологий, [S.l.], т. 25, № 2, с. 38–53, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.2.03.
12. I.I. Kagin, E.A. Simakhin, S.G. Arabian, L.N. Kessarinskiy and A.P. Durakovskiy. Development of a Software Package for the Analysis of Compromising Emanation Using LabVIEW, Proccedings of 2021 International Siberian Conference on Control and Communications (SIBCON). 2021, p. 1–5. DOI: http://dx.doi.org/10.1109/SIBCON50419.2021.9438939.
13. A. Ivanov, I. Reva, Y. Baryshnilov. Development of hardware-software complex for automatized compromising electromagnetic emanation search, Proceedings of 11th International Forum on Strategic Technology (IFOST). 2016, p. 563–565. DOI: http://dx.doi.org/10.1109/IFOST.2016.7884180.
14. I. Kubiak, A. Przybysz. DVI (HDMI) and DisplayPort digital video interfaces in electromagnetic eavesdropping process, Proceedings of 2019 International Symposium on Electromagnetic Compatibility – EMC EUROPE. 2019, p. 388–393. DOI: http://dx.doi.org/10.1109/EMCEurope.2019.8872097.
15. H. Jin, X. Rui, Z. Yunping. The Study of Reducing EMI in Power Electronic Converters Using SSFM Control Techniques, Proceedings of The 2006 4th Asia-Pacific Conference on Environmental Electromagnetics. 2006, p. 598–601. DOI: http://dx.doi.org/10.1109/CEEM.2006.258026.

REFERENCES:

[1] M.G. Kuhn. Compromising emanations of LCD TV sets, in IEEE Transaction on electromagnetic compatibility. Vol. 55, no. 3, 2013, p. 564–570. DOI: http://dx.doi.org/10.1109/TEMC.2013.2252353.

[2] P. De Meulemeester, B. Scheers, G. A. E. Vandenbosch. Differential signaling compromises video information security through AM and FM leakage emissions, in IEEE Transactions on Electromagnetic Compatibility. Vol. 62, no. 6, p. 2376–2385, 2020. DOI: http://dx.doi.org/10.1109/TEMC.2020.3000830.

[3] Ivanov A.V., Reva I.L., Ushakov A.E. Features of identification and the analysis of collateral electromagnetic radiations from USB flash drives, Proceedings of 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE). 2016, p. 156–158. DOI: http://dx.doi.org/10.1109/APEIE.2016.7806436.

[4] Durakovskiy A.P., Kessarinskiy L.N., Simakhin E.A. Detection of compromising radiation from modern data transfer interfaces using the example of high definition multimedia interface, IOP Conference Series: Materials Science and Engineering. 1069(1), 7, ISSN 1757-8981, 2021. DOI: http://dx.doi.org/10.1088/1757-899X/1069/1/012026.

[5] R. Birukawa, D. Nagata, Y. -i. Hayashi, T. Mizuki and H. Sone. The Source Estimation of Electromagnetic Information Leakage from Information Devices, 2020 XXXIIIrd General Assembly and Scientific Symposium of the International Union of Radio Science. 2020, p. 1–4. DOI: http://dx.doi.org/10.23919/URSIGASS49373.2020.9231979.

[6] T. Song, Y. Jeong, J. Yook. Modeling of Leaked Digital Video Signal and Information Recovery Rate as a Function of SNR, in IEEE Transactions on Electromagnetic Compatibility. Vol. 57, no. 2, 2015, p. 164–172. DOI: http://dx.doi.org/10.1109/TEMC.2014.2372039.

[7] Sokolov R.I., Abdullin R.R., Dolmatov D.A. Development of Synchronization System for Signal Reception and Recovery from USB-Keyboard, Proceedings of 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). 2016, p. 1–4. DOI: http://dx.doi.org/10.1109/ICIEAM.2016.7911553.

[8] Degang Sun, Di Wei, Ning Zhang, Z Lv, Xi Yin. Network transmission of hidden data using smartphones based on compromising emanations, Proceedings of 7th Asia Pacific International Symposium on Electromagnetic Compatibility (APEMC). 2016, p. 190–193. DOI: http://dx.doi.org/10.1109/APEMC.2016.7523005.

[9] P. De Meulemeester, B. Scheers, G. A. E. Vandenbosch. A Quantitative Approach to Eavesdrop Video Display Systems Exploiting Multiple Electromagnetic Leakage Channels, in IEEE Transactions on Electromagnetic Compatibility. Vol. 62, no. 3, p. 663–672, 2020. DOI: http://dx.doi.org/10.1109/TEMC.2019.2923026.

[10] P. De Meulemeester, B. Scheers, G. A. E. Vandenbosch. Reconstructing Video Images in Color Exploiting Compromising Video Emanations, Proceedings of 2020 International Symposium on Electromagnetic Compatibility - EMC EUROPE. 2020, p. 1–6. DOI: http://dx.doi.org/10.1109/EMCEUROPE48519.2020.9245775.

[11] Golyakhov Alexander A.; Durakovskiy Anatoly P.; Simakhin, Egor A. Use of generator substitution to determine the real attenuation of informative signals in the compromising emanation. IT Security (Russia), [S.l.], vol. 25, no. 2, p. 38–53, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.2.03 (in Russian).

[12] I.I. Kagin, E.A. Simakhin, S.G. Arabian, L.N. Kessarinskiy and A.P. Durakovskiy. Development of a Software Package for the Analysis of Compromising Emanation Using LabVIEW, Proccedings of 2021 International Siberian Conference on Control and Communications (SIBCON). 2021, p. 1–5. DOI: http://dx.doi.org/10.1109/SIBCON50419.2021.9438939.

[13] A. Ivanov, I. Reva, Y. Baryshnilov. Development of hardware-software complex for automatized compromising electromagnetic emanation search, Proceedings of 11th International Forum on Strategic Technology (IFOST). 2016, p. 563–565. DOI: http://dx.doi.org/10.1109/IFOST.2016.7884180.

[14] I. Kubiak, A. Przybysz. DVI (HDMI) and DisplayPort digital video interfaces in electromagnetic eavesdropping process, Proceedings of 2019 International Symposium on Electromagnetic Compatibility – EMC EUROPE. 2019, p. 388–393. DOI: http://dx.doi.org/10.1109/EMCEurope.2019.8872097.

[15] H. Jin, X. Rui, Z. Yunping. The Study of Reducing EMI in Power Electronic Converters Using SSFM Control Techniques, Proceedings of The 2006 4th Asia-Pacific Conference on Environmental Electromagnetics. 2006, p. 598–601. DOI: http://dx.doi.org/10.1109/CEEM.2006.258026.

Поступила в редакцию – 11 января 2022 г. Окончательный вариант – 02 марта 2022 г.
Received – January 11, 2022. The final version – March 02, 2022.

Сергей В. Скрыль[1], Екатерина В. Вайц[2], Сергей С. Никулин[3],
Роман А. Цой[4], Варвара А. Антонова[5]
Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет),
ул. 2-я Бауманская, 5, Москва, 105005, Россия
[1]*e-mail: skryl@bmstu.ru, https://orcid.org/0000-0002-4309-6255*
[2]*e-mail: vaitcev@yandex.ru, https://orcid.org/0000-0002-4629-6252*
[3]*e-mail: nikcc@mail.ru, https://orcid.org/0000-0002-4723-7844*
[4]*e-mail: romabmstu@bmstu.ru, https://orcid.org/0000-0002-2454-3224*
[5]*e-mail: varvara_zi@mail.ru, https://orcid.org/0000-0002-6467-5002*

ТЕХНОЛОГИЯ SOFT TEMPEST КАК ОБЪЕКТ ФУНКЦИОНАЛЬНОГО МОДЕЛИРОВАНИЯ

DOI: http://dx.doi.org/10.26583/bit.2022.1.11

Аннотация. Данная статья посвящена представлению технологии программно-управляемого побочного электромагнитного излучения (технологии Soft Tempest (ST)) и процессов противодействия утечке информации по ST-каналу в терминах функционального моделирования. Подобное представление является средством первичной формализации действий нарушителя по внедрению вредоносного программного обеспечения (ВПО) в рабочую среду СВТ для инициализации побочных электромагнитных излучений (ПЭМИ) от электронного оборудования СВТ, а также противодействию утечке информации по каналу рассматриваемого типа. Представлен общий механизм декомпозиции целевых функций «Перехват нарушителем информативных сигналов СВТ по ST-каналу» и «Противодействие утечке информации по ST-каналу». Обосновываются классификационные основания для трехуровневой детализации данных целевых функций. Приводятся результаты детализации действий нарушителя на отдельные этапы, реализуемые мероприятия по противодействию утечке информации, выполняемые нарушителем процедуры, принимаемые меры противодействия и соответствующие этим процедурам и мерам функции. Полученные результаты являются предпосылкой для формализованного представления описываемых процессов в терминах Марковских процессов и разработки математических моделей, соответствующих временных и вероятностных характеристик для количественной оценки возможностей нарушителя по реализации угроз перехвата побочных электромагнитных излучений от электронного оборудования СВТ, вызванных воздействием ВПО.
Ключевые слова: технология Soft Tempest, ST-канал утечки информации, перехват информативных сигналов, противодействие утечке информации по ST-каналу, программно-управляемое побочное электромагнитное излучение.
Для цитирования: СКРЫЛЬ, Сергей В. и др. ТЕХНОЛОГИЯ SOFT TEMPEST КАК ОБЪЕКТ ФУНКЦИОНАЛЬНОГО МОДЕЛИРОВАНИЯ. Безопасность информационных технологий, [S.l.], т. 29, № 1, p. 125–144, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1412. DOI: http://dx.doi.org/10.26583/bit.2022.1.11.

Sergey V. Skryl[1], Ekaterina V. Vaitc[2], Sergey S. Nikulin[3], Roman A. Tsoy[4],
Varvara A. Antonova[5]
Bauman Moscow State Technical University (National Research University),
2nd Bauman Str., 5, Moscow, 105005, Russia
[1]*e-mail: skryl@bmstu.ru, https://orcid.org/0000-0002-4309-6255*
[2]*e-mail: vaitcev@yandex.ru, https://orcid.org/0000-0002-4629-6252*
[3]*e-mail: nikcc@mail.ru, https://orcid.org/0000-0002-4723-7844*
[4]*e-mail: romabmstu@bmstu.ru, https://orcid.org/0000-0002-2454-3224*
[5]*e-mail: varvara_zi@mail.ru, https://orcid.org/0000-0002-6467-5002*

Soft tempest technology as an object of functional modeling

DOI: http://dx.doi.org/10.26583/bit.2022.1.11

Abstract. This article focuses on presenting the software-controlled transient electromagnetic pulse emanation technology (Soft Tempest (ST) technology) and the ST-channel information leakage counteraction in terms of functional modeling. Such a representation is a means of primary formalization of the actions of the intruder to prepare the implementation malicious software into the CT working environment to initiate a transient electromagnetic pulse emanation (TEMPE) from electronic equipment of CT and also formalization of countering of information leakage via reviewed channel. The general mechanism of decomposition of the target functions «Intruder interception of informative signals of CE via ST-channel» and «Counteracting information leakage via the ST-channel» is presented in this article. The classification basis for the three-level detailing of these target functions is substantiated. The report provides the results of detailing the actions of the intruder into certain stages, the ongoing activities to counteract information leakage, the processes taken by the intruder, taken countermeasures and the functions corresponding to these processes and countermeasures. The results thus obtained are a prerequisite for the formalized representation of the processes described in terms of Markov processes and the development of mathematical models of the related temporal and stochastic characteristics to quantitatively measure the ability of the intruder to realize the threats of interception of a TEMPE from the electronic equipment of CT, caused by malware.

Keywords: Soft Tempest technology, information leakage, interception of informative signals of computers technique (CT) via the ST-channel, software-controlled transient electromagnetic pulse emanation.

For citation: SKRYL, Sergey V. et al. Soft tempest technology as an object of functional modeling. IT Security (Russia), [S.l.], v. 29, n. 1, p. 125–144, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1412. DOI: http://dx.doi.org/10.26583/bit.2022.1.11.

Введение

Анализ ретроспектив технической разведки (ТР), как способа перехвата информативных сигналов физических полей, содержащих конфиденциальную информацию; и перспектив дальнейшего совершенствования ТР позволяет выявить устойчивую тенденцию к целенаправленному совершенствованию способов и средств перехвата компьютерной информации по каналам побочных электромагнитных излучений (ПЭМИ) [1–4]. Это обусловлено, главным образом совершенствованием технологии электронного документооборота, в результате которого огромное количество конфиденциальной информации аккумулируется в электронных документах. В отличие от традиционного способа несанкционированного получения конфиденциальной информации техническими средствами разведки – путем перехвата отдельных речевых сообщений, перехват электронного документа, позволяет обеспечить высокую степень целостности перехваченной информации. Вместе с тем, существуют и специфичные технические каналы утечки информации, комбинирующие программные способы воздействия на информационную среду и способы перехвата информативных сигналов физических полей [5]. Подобная технология перехвата компьютерной информации получила широкую известность как технология скрытой передачи данных по каналу ПЭМИ с помощью программных средств – Soft Tempest (ST) [5]. В отечественной литературе по технической защите информации подобный способ перехвата компьютерной информации получил название программно-управляемое побочное электромагнитное излучение. ST-технология, по своей сути, есть разновидность компьютерной стеганографии, т.е. метода скрытной передачи полезного сообщения в видео, аудио, графических и текстовых файлах [6].

Высокая скрытность такого рода канала утечки информации обусловила необходимость его исследования с целью научного обоснования требований к характеристикам применяемых способов и средств противодействия данному, весьма специфичному, виду технической разведки.

Следует отметить, что существующая практика обоснования подобного рода требований, вследствие своей эмпирической природы, не обеспечивает обоснованность этих решений.

Очевидно, что обоснованность решений относительно направлений совершенствования механизмов защиты информации от утечки по ST-каналу должна основываться на адекватной оценке возможностей противодействия утечке.

Следует отметить, что применение с этой целью существующего методического аппарата оценки характеристик безопасности информационных технологий, связано с рядом проблем. Наиболее значимыми из них являются:

1) отсутствие формальных оснований для представления угрозы утечки информации по ST-каналу как действий нарушителя по ее реализации, и как следствие, ограниченное число состояний, характеризующих такого рода угрозу;

2) необходимость оценки комплексного влияния на процесс противодействия утечке информации по ST-каналу двух, существенно различных по своей природе, механизмов предотвращения такого рода угрозы – антивирусного и технического контроля.

3) отсутствие математической интерпретации ряда случайных событий, характеризующих динамику угрозы утечки информации по ST-каналу и его обнаружения средствами защиты от такого рода угроз.

Это не позволяет использовать существующий методический аппарат оценки характеристик безопасности информационных технологий для адекватной оценки возможностей по реализации угроз утечки информации по ST-каналу и, как следствие, в качестве инструмента формирования обоснованных решений относительно характеристик применяемых способов и средств противодействия.

Целью данной статьи является обоснование возможностей преодоления обстоятельств, обусловленных первыми двумя, из перечисленных выше проблем за счет применения методологии функционального моделирования, позволяющей определить все возможные состояния как процесса реализации угроз утечки информации по ST-каналу, так и процесса противодействия данному виду технической разведки.

1. Особенности формирования ST-канала утечки информации

Исследования по разработке тестовых сигналов для анализа интерфейсов средств вычислительной техники (СВТ), выполненные Маркусом Куном (Markus G. Kuhn) в 1998 г. в лаборатории Кембриджского университета, продемонстрировали возможность формирования нового типа технического канала утечки информации. Суть исследований состояла в том, что объект воздействия (СВТ) «заражается» вредоносной программой со специализированными возможностями. Такого рода программа ищет необходимую информацию в памяти СВТ и путем обращения к различным его устройствам вызывает появление ПЭМИ. Например, вредоносная программа может встраивать сообщение в сигнал монитора, при этом пользователь не подозревает, что в изображение на экране монитора вставлены определенные текстовые сообщения или изображения. С помощью разведывательного приемника обеспечивается перехват паразитного излучения монитора и выделение требуемого полезного сигнала.

Высокая эффективность ST-технологии, как разновидности угроз безопасности компьютерной информации, достигается за счет скрытности работы вредоносной программы.

В отличие от традиционного способа использования вредоносных программ в качестве источника угроз нарушения конфиденциальности информации в компьютерной сети [7], применение ST-технологии не предполагает рассылку несанкционированного

скопированных данных по сети, что позволяет в течение длительного времени не обнаруживать утечку информации соответствующими антивирусными средствами. Поэтому, вредоносные программы, использующие в качестве физической среды для передачи данных ПЭМИ электронного оборудования СВТ, могут работать годами, не обнаруживая себя.

В случае автономной работы СВТ ST-технология является для нарушителя единственным способом получения конфиденциальной информации, обрабатываемой данным средством.

В 2001 г. Эрик Тиле (Erik Thiele), основываясь на работе Маркуса Куна [8] представил программу Tempest for Eliza, позволяющую использовать VGA интерфейс в качестве генератора радиосигнала с амплитудной модуляцией.

Качественное развитие технология передачи данных за счёт ПЭМИ получила в 2014 г., когда Мордехай Гури (Mordechai Guri) с коллегами представили работу AirHopper [9]. В работе реализована возможность передачи информации по каналу ПЭМИ, с возможностью приема информации на встроенный приемник мобильного телефона или смартфона.

Уильям Энтрикен (William Entriken) воодушевившись работами Гури опубликовал программное обеспечение (ПО), позволяющее осуществлять амплитудную модуляцию (АМ) излучения шины памяти (I/O bus clock) при обмене данными между CPU и RAM.

Авторы исследования смогли добиться скорости передачи порядка 1000 бит/с на расстоянии 2,6 м, при использовании SDR-приемника.

В августе 2015 г. Гури представил программное обеспечение GSMem, формирующее радиоканал передачи данных на частотах сетей сотовой связи GSM, UMTS и LTE, а также в диапазоне частот Wi-Fi. Данное ПО использует специфические инструкции процессора, непрерывно изменяя несущие частоты многоканальной памяти. Авторам удалось добиться стабильной скорости передачи 1000 бит/с на расстоянии в 2 м, прием осуществлялся на мобильные телефоны.

В 2016 г. Мордехай Гури представил способ передачи информации за счёт ПЭМИ USB-интерфейса, добившись скорости 80 байт/с в процессе манипуляции несущей частоты интерфейса при передаче данных по нему. В качестве антенны выступал сам интерфейс и подключенный к нему флеш-накопитель. Метод передачи получил название USBee [10].

Стоит отметить, что исследования Гури не ограничились формированием радиоканалов, так на данный момент представлены способы передачи информации от изолированного от внешних подключений СВТ с помощью:

– световых волн мерцания светодиода во время работы жесткого диска 20 бит/с при использовании обычной видеокамеры для фиксации;

– звуковых волн, формируемых шумом вентилятора 900 байт/ч;

– периодически появляющихся кадров низкой контрастности от современных LCD мониторов, которые могут быть восстановлены при помощи камеры;

– термальных флуктуаций СВТ (с помощью ПО BitWhisper до 10 бит/час на расстоянии полуметра) [11].

Таким образом, наличие в составе СВТ аппаратных составляющих, способных излучать ПЭМИ и возможность программного управления режимами работы СВТ, обеспечивают модуляцию этих излучений информационными сигналами. В результате формируется ST-канал утечки информации.

В табл.1 приводится характеристика известных способов реализации ST-технологии.

Таблица 1. Сравнение известных способов передачи информации посредством модуляции ПЭМИ от СВТ

Наименование способа передачи	**Источник излучения**	**Достигнутая скорость**	**Порядок дальности приема**
Markus G. Kuhn Soft Tempest, 1999 г	Электронно-лучевая трубка	-	1 км
AirHopper, 2014 г.	Интерфейс VGA	8 байт/с	100 м
GSMem, 2015 г.	Системная шина данных (front-side)	1000 бит/с	20 м
USBee, 2016 г.	USB интерфейс	80 байт/с	30 м

Возможность модуляции ПЭМИ информацией, обрабатываемой СВТ, но непосредственно не передающейся в излучающем интерфейсе в нормальном режиме работы, является ключевой особенностью и главным отличием ST-технологии от классического перехвата информационных сигналов ПЭМИ. Их сравнение представлено в табл. 2.

Таблица 2. Сравнение классического перехвата информационных сигналов ПЭМИ и ST-технологии

	Классический перехват информационных сигналов ПЭМИ	**ST-технология**
Носитель информации	ПЭМИ	ПЭМИ
Источник сигнала	Интерфейс, участвующий в обработке информации	Любой интерфейс, излучающий ПЭМИ и допускающий программное управление
Передаваемая (излучаемая) информация	Информация, обрабатываемая излучающим интерфейсом	Любая информация ограниченного доступа, к которой имеет доступ программа, формирующая ПЭМИ
Скорость передачи информации	Определяется длительностью импульса тактовой частоты излучающего интерфейса	Определяется временем изменения параметров интерфейса
Тип передаваемого сигнала	Широкополосный	Узкополосный
Условия формирования технического канала утечки информации	Зона, в которой возможен перехват ПЭМИ с помощью разведывательного приемника, с последующей расшифровкой, содержащейся в них информации, больше расстояния до границы контролируемой зоны	Программная закладка в СВТ

Результаты экспериментальных исследований по формированию канала передачи данных, основанного на ST-технологии некоторых интерфейсов СВТ представлены в табл. 3.

Таблица 3. Сравнение каналов передачи информации основанных на ST-технологии интерфейсов СВТ

Излучающий ST-интерфейс	**Модуляция**	**Экспериментально достигнутая дальность приема без когерентного накопления**	**Экспериментально достигнутая скорость передачи информации**
VGA	ФМ, ЧМ	80 м	400 бит/с
DVI, HDMI	АМ	6 м	20 бит/с
PCI, PCI-E	ЧМ	10 м	100 бит/с
FSB	ЧМ	7 м	100 бит/с
GPU	АМ	1 м	1 бит/с

Таким образом, очевидно, что ST-технология, как объект противодействия техническим разведкам, нуждается в глубоком изучении.

2. Формализованное представление действий нарушителя по перехвату информативных сигналов СВТ по ST-каналу

Обоснование требований к способам и средствам противодействия утечке информации по ST-каналу предполагает наличие соответствующего методического аппарата, позволяющего адекватно оценить как характеристики такого рода канала, так и характеристики средств противодействия утечке. Рассмотрим возможность применения для решения данной проблемы классической методологии исследования – теории моделирования.

К настоящему времени в методологии моделирования в целом и в теории и практике противодействия техническим разведкам, в частности, сформирована довольно обширная методическая база функционального моделирования исследуемых процессов, как средства их первичной формализации [12]. При этом выделяются две наиболее распространенные формы представления этих моделей: представление в виде функциональных диаграмм [13] и представление в виде графов [14]. Обе формы представления позволяют отразить все детали функциональных компонент исследуемых процессов в рамках иерархии их функциональной декомпозиции.

Функциональные диаграммы представляют собой довольно наглядное средство интерпретации всех деталей информационных процессов со сложной функциональной структурой: внутренний интерфейс функциональных компонент, интерфейс с внешней информационной средой, условия реализации исследуемых информационных процессов и используемые при этом ресурсы. Вместе с тем опыт применения методического аппарата для функционального моделирования информационных процессов, представляемых как отдельные состояния, реализуемые в однотипной информационной среде с ограниченной номенклатурой средств, позволяет утверждать о существенной избыточности функциональных диаграмм как инструмента первичной формализации.

Этого недостатка лишено представление этих процессов в виде декомпозиционной структуры графов. Подобное функциональное описание содержит лишь необходимые для идентификации функций параметры: перечень реализуемых состояний, характеристики нахождения процессов в этих состояниях и порядок смены состояний. Все эти параметры на каждом из уровней функциональной декомпозиции исследуемого процесса представляются в виде графа. Как и в случае функционального описания с помощью функциональных диаграмм представление исследуемых процессов в виде декомпозиционной структуры графов дает возможность отразить функциональную иерархию этих процессов, получаемую в результате декомпозиции реализуемых функций.

Проиллюстрируем эти возможности для формализации ST-технологии.

В основе такой иерархии лежит представление целевой функции «Перехват нарушителем информативных сигналов СВТ по ST-каналу» в наиболее обобщенном виде – в виде одного состояния, реализующего данную целевую функцию. Подобное представление в терминах декомпозиционной структуры графов определяется как концептуальная функциональная модель процессов, связанных реализацией такого рода угрозы безопасности информации (функциональная модель нулевого уровня).

Детализация концептуальной функциональной модели этих процессов позволяет выявить набор подфункций, реализующих вышеуказанную целевую функцию. Этот набор образует первый уровень декомпозиционной структуры графов, описывающих процессы реализации ST-технологии.

Выявление набора подфункций для любой функции исследуемых процессов позволяет формировать следующие уровни их функциональной иерархии.

Декомпозиция может быть завершена в том случае, когда набор подфункций может быть описан терминами цепей Маркова [15].

При формировании функциональной модели процессов перехвата нарушителем информативных сигналов СВТ по ST-каналу воспользуемся результатами анализа практики реализации такого рода угроз безопасности информации.

Первый уровень декомпозиции целевой функции «Перехват нарушителем информативных сигналов СВТ по ST-каналу» составляют подфункции подготовки к реализации такого рода угрозы, внедрения вредоносного кода, его распространение в рабочей среде СВТ, обнаружение и перехват информативных сигналов ПЭМИ от электронного оборудования СВТ, а также обработки перехваченной информации [16]. Данные подфункции следует рассматривать как этапы реализации целевой функции (рис. 1):

$Э_1$ – этап подготовки к перехвату информативных сигналов СВТ по ST-каналу;

$Э_2$ – этап внедрения вредоносного кода в рабочую среду СВТ;

$Э_3$ – этап инициализации вредоносным кодом ПЭМИ от электронного оборудования СВТ;

$Э_4$ – этап обнаружения ПЭМИ от электронного оборудования СВТ;

$Э_5$ – этап перехвата информативных сигналов ПЭМИ от электронного оборудования СВТ;

$Э_6$ – этап обработки информативных сигналов от электронного оборудования СВТ.

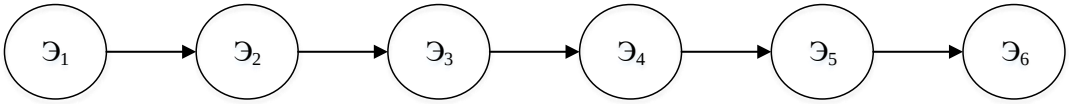


Рис. 1. Декомпозиционное представление целевой функции «Перехват нарушителем информативных сигналов СВТ по ST-каналу»
Fig. 1. Decomposition view of the target function «Intruder interception of informative signals of CT via ST-channel»

Второй уровень декомпозиции целевой функции «Перехват нарушителем информативных сигналов СВТ по ST-каналу» образуется путем детализации действий нарушителя, выполняемых им в процессе реализации этапов $Э_1$–$Э_6$. Соответствующие данному уровню действия следует рассматривать как процедуры реализации указанных этапов.

К процедурам, реализующим этап $Э_1$ подготовки к перехвату информативных сигналов СВТ по ST-каналу, относятся (рис. 2):

$П_{11}$ – процедура сбора информации об объекте угрозы утечки информации по ST-каналу;

$П_{12}$ – процедура разработки соответствующего вредоносного кода.

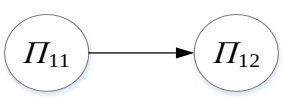


Рис. 2. Декомпозиционное представление этапа подготовки к перехвату информативных сигналов СВТ по ST-каналу
Fig. 2. Decomposition view of the stage of preparation for the interception of informative signals of computer equipment via ST-channel

К процедурам, реализующим этап $Э_2$ внедрения вредоносного кода в рабочую среду СВТ, относятся (рис. 3):

$П_{21}$ – процедура получения доступа к рабочей среде СВТ;

$П_{22}$ – процедура внедрения вредоносного кода в рабочую среду СВТ;

$П_{23}$ – процедура сокрытия работы вредоносного кода.

Рис. 3. Декомпозиционное представление этапа внедрения вредоносного кода в рабочую среду СВТ

Fig. 3. Decomposition view of the stage of the malware implementation in the working environment of CT

К процедурам, реализующим этап $Э_3$ инициализации вредоносным кодом ПЭМИ от электронного оборудования СВТ, относятся (рис. 4):

$П_{31}$ – процедура определения вредоносным кодом доступных интерфейсов передачи данных в рабочей среде СВТ;

$П_{32}$ – процедура обнаружения информации, являющейся целью перехвата;

$П_{33}$ – процедура кодирования информации, являющейся целью перехвата;

$П_{34}$ – процедура формирования программного инструментария для реализации воздействия на интерфейс передачи данных в рабочей среде СВТ;

$П_{35}$ – процедура реализации воздействия на интерфейс передачи данных в рабочей среде СВТ.

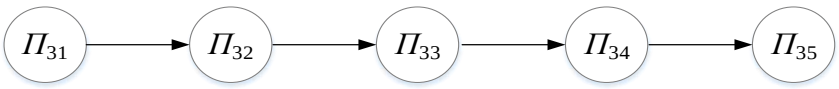


Рис. 4. Декомпозиционное представление этапа инициализации вредоносным кодом ПЭМИ от электронного оборудования СВТ

Fig. 4. Decomposition view of the stage the malware initiation of a transient electromagnetic pulse emanation (TEMPE) from electronic equipment of CT

К процедурам, реализующим этап $Э_4$ обнаружения ПЭМИ от электронного оборудования СВТ, относятся (рис. 5):

$П_{41}$ – процедура определения частотного диапазона для обнаружения информативных сигналов ПЭМИ от электронного оборудования СВТ;

$П_{42}$ – процедура верификации обнаруженных информативных сигналов ПЭМИ от электронного оборудования СВТ.

Рис. 5. Декомпозиционное представление этапа обнаружения ПЭМИ от электронного оборудования СВТ

Fig. 5. Decomposition view of the stage of detection of the TEMPE from electronic equipment of CT

К процедурам, реализующим этап $Э_5$ перехвата информативных сигналов ПЭМИ от электронного оборудования СВТ, относятся (рис. 6):

$П_{51}$ – процедура настройки технического средства разведки (ТСР) для приема информативных сигналов ПЭМИ от электронного оборудования СВТ;

$П_{52}$ – процедура приема и записи информативных сигналов ПЭМИ от электронного оборудования СВТ.

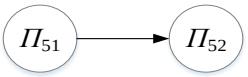


Рис. 6. Декомпозиционное представление этапа перехвата информативных сигналов ПЭМИ от электронного оборудования СВТ
Fig. 6. Decomposition view of the stage interception of informative signals of the TEMPE from electronic equipment of CT

К процедурам, реализующим этап $Э_6$ обработки информативных сигналов от электронного оборудования СВТ, относятся (рис. 7):

$П_{61}$ – процедура демодуляции перехваченных информативных сигналов ПЭМИ от электронного оборудования СВТ;

$П_{62}$ – процедура обработки перехваченной информации с целью обеспечения ее целостности.

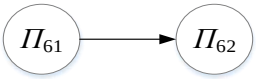


Рис. 7. Декомпозиционное представление этапа обработки информативных сигналов от электронного оборудования СВТ
Fig. 7. Decomposition view of the stage of processing of informative signals of the TEMPE from electronic equipment of CT

Третий уровень декомпозиции целевой функции «Перехват нарушителем информативных сигналов СВТ по ST-каналу» образуется путем детализации действий, выполняемых в процессе реализации процедур $П_{11}$–$П_{62}$. Соответствующие данному уровню действия следует рассматривать как функции, реализующие указанные процедуры.

К функциям, реализующим процедуру сбора информации об объекте угрозы утечки информации по ST-каналу (процедуру $П_{11}$), относятся (рис. 8):

$Ф_{111}$ – функция определения режимов использования СВТ для сбора информации об объекте угрозы;

$Ф_{112}$ – функция сбора информации о сотрудниках, допущенных к СВТ;

$Ф_{113}$ – функция сбора информации о времени работы сотрудников с СВТ;

$Ф_{114}$ – функция сбора информации о средствах защиты информации, установленных на СВТ;

$Ф_{115}$ – функция сбора информации о ПО, установленном на СВТ;

$Ф_{116}$ – функция определения возможностей по внедрению вредоносного кода.

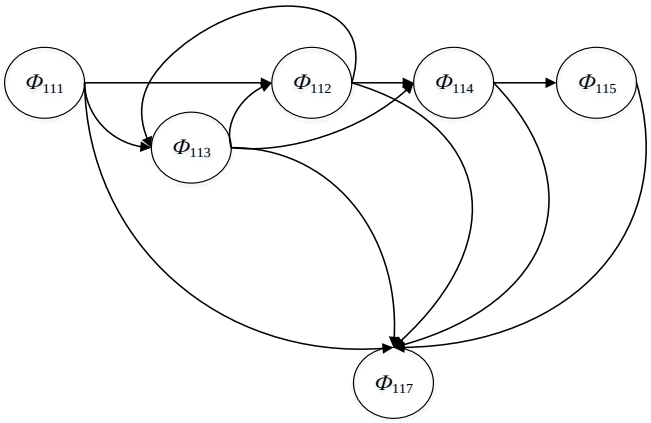


Рис. 8. Декомпозиционное представление процедуры сбора информации об объекте угрозы утечки информации по ST-каналу
Fig. 8. Decomposition view of the procedure for information gathering on the object of information leak threat via ST-channel

К функциям, реализующим процедуру разработки соответствующего вредоносного кода (процедуру $П_{12}$), относятся (рис. 9):

$Ф_{121}$ – функция определения инструментов вредоносного воздействия на электронное оборудование СВТ через его рабочую среду;

$Ф_{122}$ – функция выявления уязвимостей механизмов защиты информации в СВТ;

$Ф_{123}$ – функция использования выявленных уязвимостей.

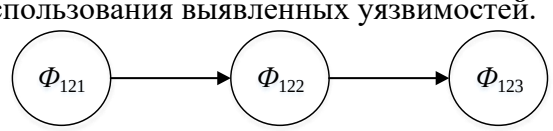


Рис. 9. Декомпозиционное представление процедуры разработки соответствующего вредоносного кода
Fig. 9. Decomposition view of the procedure for developing the appropriate malware

К функциям, реализующим процедуру получения доступа к рабочей среде СВТ (процедуру $П_{21}$), относятся (рис. 10):

$Ф_{211}$ – функция использования доступа, предоставленного третьей стороне;

$Ф_{212}$ – функция использования доверенного носителя информации, содержащего вредоносное ПО;

$Ф_{213}$ – функция несанкционированного подключения внешних устройств.

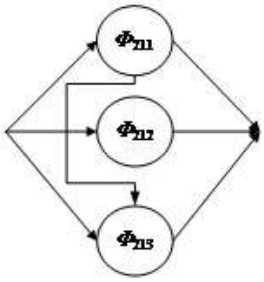


Рис. 10. Декомпозиционное представление процедуры получения доступа к рабочей среде СВТ
Fig. 10. Decomposition view of the procedure for gaining access to the CT workspace

К функциям, реализующим процедуру внедрения вредоносного кода в рабочую среду СВТ (процедуру $П_{22}$), относятся (рис. 11):

$Ф_{221}$ – функция переноса вредоносного кода в рабочую среду СВТ через съемные носители информации;

$Ф_{222}$ – функция переноса вредоносного кода в рабочую среду СВТ через программные компоненты, используя возможности удаленного доступа;

$Ф_{223}$ – функция переноса вредоносного кода в рабочую среду СВТ посредством физического соединения с другими устройствами, входящими в состав СВТ.

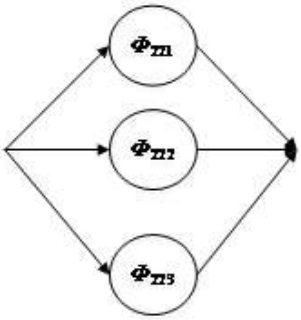


Рис. 11. Декомпозиционное представление процедуры внедрения вредоносного кода в рабочую среду СВТ
Fig. 11. Decomposition view of the procedure for the malware implementation in the working environment of CT

К функциям, реализующим процедуру сокрытия работы вредоносного кода (процедуру $П_{23}$), относятся (рис. 12):

$Ф_{231}$ – функция программного анализа рабочей среды СВТ;

$Ф_{232}$ – функция адаптации вредоносного кода в рабочей среде СВТ.

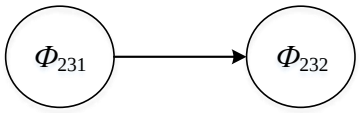


Рис. 12. Декомпозиционное представление процедуры сокрытия работы вредоносного кода
Fig. 12. Decomposition view of the procedure for malware operation concealment

К функциям, реализующим процедуру определения доступных интерфейсов передачи данных в рабочей среде СВТ (процедуру $П_{31}$), относятся (рис. 13):

$Ф_{311}$ – функция проверки наличия доступных интерфейсов передачи данных в рабочей среде СВТ;

$Ф_{312}$ – функция проверки возможности получения доступа к выбранному интерфейсу передачи данных в рабочей среде СВТ.

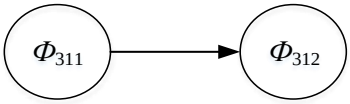


Рис. 13. Декомпозиционное представление процедуры определения доступных интерфейсов передачи данных в рабочей среде СВТ
Fig. 13. Decomposition view of the procedure for identification of available data transmission interfaces in the CT workspace

К функциям, реализующим процедуру обнаружения информации, являющейся целью перехвата (процедуру $П_{32}$), относятся (рис. 14):

$Ф_{321}$ – функция поиска необходимой информации в соответствии с установленными нарушителем параметрами рабочей среды СВТ;

$Ф_{322}$ – функция попытки получения доступа к информации, являющейся целью перехвата, в рабочей среде СВТ.

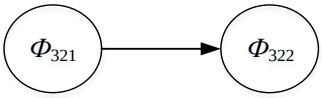


Рис. 14. Декомпозиционное представление процедуры обнаружения информации, являющейся целью перехвата
Fig. 14. Decomposition view of the procedure for detecting information that is the interception target

К функциям, реализующим процедуру кодирования найденной в рабочей среде СВТ информации (процедуру $П_{33}$), относятся (рис. 15):

$Ф_{331}$ – функция подготовки найденной информации к кодированию для выбранного интерфейса передачи данных в рабочей среде СВТ;

$Ф_{332}$ – функция преобразования найденной информации в соответствии с выбранной кодировкой.

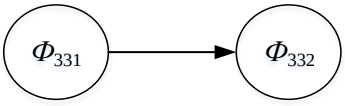


Рис. 15. Декомпозиционное представление процедуры кодирования найденной в рабочей среде СВТ информации
Fig. 15. Decomposition view of the coding procedure for the found information in the CT workspace

К функциям, реализующим процедуру формирования данных для воздействия на интерфейс передачи данных в рабочей среде СВТ (процедуру $П_{34}$), относятся (рис. 16):

$Ф_{341}$ – функция подготовки кодированной информации к формированию пакета данных;

$Ф_{342}$ – функция формирования пакета данных.

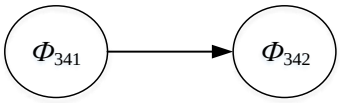


Рис. 16. Декомпозиционное представление процедуры формирования программного инструментария для реализации воздействия на интерфейс передачи данных в рабочей среде СВТ
Fig. 16. Decomposition view of the procedure for forming a software toolkit to influence the data transfer interface in CT work environment

К функциям, реализующим процедуру реализации воздействия на интерфейс передачи данных в рабочей среде СВТ (процедуру $П_{35}$), относятся (рис. 17):

$Ф_{351}$ – функция получения доступа к интерфейсу передачи данных в рабочей среде СВТ;

$Ф_{352}$ – функция циклической отправки пакета данных по интерфейсу передачи данных в рабочей среде СВТ.

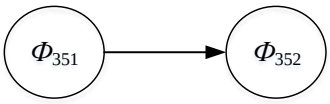


Рис. 17. Декомпозиционное представление процедуры реализации воздействия на интерфейс передачи данных в рабочей среде СВТ
Fig. 17. Decomposition view of the procedure for realization of the impact on the data transfer interface in the CT work environment

К функциям, реализующим процедуру определения частотного диапазона для обнаружения информативных сигналов ПЭМИ от электронного оборудования СВТ (процедуру $П_{41}$), относятся (рис. 18):

$Ф_{411}$ – функция сканирования спектра электромагнитных сигналов в заданном диапазоне частот;

$Ф_{412}$ – функция обнаружения ПЭМИ в заданном частотном диапазоне;

$Ф_{413}$ – функция определения несущей частоты ПЭМИ.

Рис. 18. Декомпозиционное представление процедуры определения частотного диапазона для обнаружения информативных сигналов ПЭМИ от электронного оборудования СВТ
Fig. 18. Decomposition view of the procedure for determining the frequency range for detecting informative TEMPE signals from electronic equipment of CT

К функциям, реализующим процедуру верификации обнаруженных информативных сигналов ПЭМИ от электронного оборудования СВТ (процедуру $П_{42}$), относятся (рис. 19):

$Ф_{421}$ – функция анализа спектра обнаруженного ПЭМИ на несущей частоте;

$Ф_{422}$ – функция верификации обнаруженного ПЭМИ на несущей частоте.

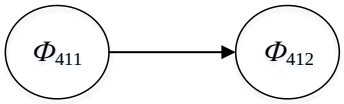


Рис. 19. Декомпозиционное представление процедуры верификации обнаруженных информативных сигналов ПЭМИ от электронного оборудования СВТ
Fig. 19. Decomposition view of the procedure for verification of detected informative TEMPE signals from electronic equipment of CT

К функциям, реализующим процедуру настройки ТСР для приема информативных сигналов ПЭМИ от электронного оборудования СВТ (процедуру $П_{51}$), относятся (рис. 20):

$Ф_{511}$ – функция выбора оптимальной измерительной приемной антенны в соответствии с частотным диапазоном;

$Ф_{512}$ – функция выбора оптимального измерительного приемника, в соответствии с заданным частотным диапазоном и полосой пропускания сигнала.

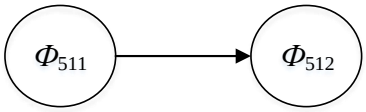


Рис. 20. Декомпозиционное представление процедуры настройки ТСР для приема информативных сигналов ПЭМИ от электронного оборудования СВТ
Fig. 20. Decomposition view of the procedure for setting up a technical intelligence device (TID) to receive informative TEMPE signals from electronic equipment of CT

К функциям, реализующим процедуру приема и записи информативных сигналов ПЭМИ от электронного оборудования СВТ (процедуру $П_{52}$), относятся (рис. 21):

$Ф_{521}$ – функция приема входного электромагнитного сигнала;

$Ф_{522}$ – функция накопления IQ-данных сигналов ПЭМИ;

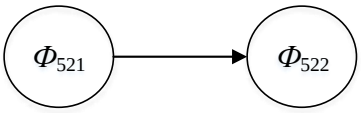


Рис. 21. Декомпозиционное представление процедуры приема и записи информативных сигналов ПЭМИ от электронного оборудования СВТ
Fig. 21. Decomposition view of the procedure for receiving and recording of informative TEMPE signals from electronic equipment of CT

К функциям, реализующим процедуру демодуляции перехваченных информативных сигналов ПЭМИ от электронного оборудования СВТ (процедуру $П_{61}$), относятся (рис. 22):

$Ф_{611}$ – функция обработки IQ-данных;

$Ф_{612}$ – функция восстановления поврежденных данных.

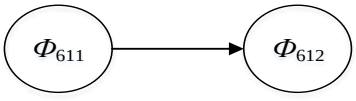


Рис. 22. Декомпозиционное представление процедуры демодуляции перехваченных информативных сигналов ПЭМИ от электронного оборудования СВТ
Fig. 22. Decomposition view of the procedure for the demodulation of intercepted informative TEMPE signals from electronic equipment of CT

К функциям, реализующим процедуру обработки перехваченной информации с целью обеспечения ее целостности (процедуру $П_{62}$), относятся (рис. 23):

$Ф_{621}$ – функция проверки целостности информации;

$Ф_{622}$ – функция ознакомления с информацией.

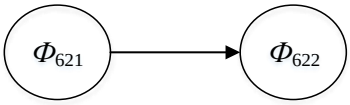


Рис. 23. Декомпозиционное представление процедуры обработки перехваченной информации с целью обеспечения ее целостности

Fig. 23. Decomposition view of the procedure for processing intercepted information in order to ensure its integrity

3. Формализованное представление мер противодействия утечке информации по ST-каналу

Проиллюстрируем возможности функционального моделирования для формализации процессов противодействия утечки информации по ST-каналу.

Основу данной функциональной модели составляет декомпозиционное представление целевой функции «Противодействие утечке информации по ST-каналу». В наиболее обобщенном виде функциональная модель представляется в виде одного состояния, реализующего указанную целевую функцию. Подобное представление в терминах декомпозиционной структуры графов определяется как функциональная модель нулевого уровня.

Детализация функциональной модели целевой функции позволяет выявить набор соответствующих подфункций, которые будут составлять первый уровень декомпозиционной структуры графов, описывающих процессы противодействия утечки информации по ST-каналу.

Выявление набора подфункций для любой функции описывающих исследуемые процессы позволяет формировать следующие уровни их функциональной иерархии.

Процесс функциональной декомпозиции завершается тогда, когда набор подфункций может быть представлен Марковским процессом [15].

Первый уровень декомпозиции целевой функции «Противодействие утечке информации по ST-каналу» составляют подфункции, связанные с изменением программно-аппаратной конфигурации электронного оборудования СВТ, его инструментальной проверкой и техническим контролем эффективности защиты информации от утечки по ST-каналу. Данные подфункции рассматриваются как мероприятия по противодействию утечке информации по ST-каналу (рис. 24):

M_1 – мероприятия по изменению программно-аппаратной конфигурации электронного оборудования СВТ;

M_2 – мероприятия по инструментальной проверке электронного оборудования СВТ;

M_3 – мероприятия по техническому контролю эффективности защиты информации от утечки по ST-каналу.

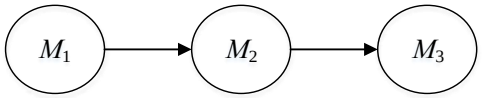


Рис. 24. Декомпозиционное представление целевой функции «Противодействие утечке информации по ST-каналу»

Fig. 24. Decomposition view of the target function «Counteracting information leakage through the ST channel»

Второй уровень декомпозиции целевой функции «Противодействие утечке информации по ST-каналу» образуется путем детализации мероприятий M_1–M_3. Соответствующие данному уровню подфункции рассматриваются как меры, предпринимаемые для реализации указанных мероприятий.

К мерам, предпринимаемым для реализации мероприятий M_1 по изменению программно-аппаратной конфигурации электронного оборудования СВТ, относятся (рис. 25):

E_{11} – меры по изменению конфигурации электронного оборудования СВТ;

E_{12} – меры по замене импортного программно-аппаратного обеспечения СВТ на отечественное.

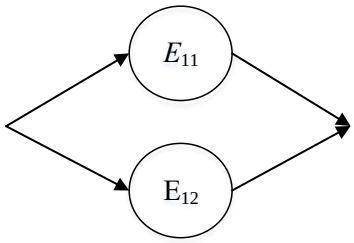


Рис. 25. Декомпозиционное представление мероприятий по изменению программно-аппаратной конфигурации электронного оборудования СВТ
Fig. 25. Decomposition view of the activities for hardware and software configuration changes to electronic equipment of CT

К мерам, предпринимаемым для реализации мероприятий M_2 по инструментальной проверке электронного оборудования СВТ, относятся (рис. 26):

E_{21} – меры по проведению исследований на соответствие требованиям по безопасности информации;

E_{22} – меры по проведению дополнительных исследований.

Рис. 26. Декомпозиционное представление мероприятий по инструментальной проверке электронного оборудования СВТ
Fig. 26. Decomposition view of activities for the instrumental verification of the electronic equipment of CT

К мерам, предпринимаемым для реализации мероприятий M_3 по техническому контролю эффективности защиты информации от утечки по ST-каналу, относятся (рис. 27):

E_{31} – меры пассивной защиты информации;

E_{32} – меры активной защиты информации;

E_{33} – меры, реализуемые с целью оценки эффективности защиты информации от утечки по ST-каналу в соответствии требованиями по безопасности информации;

E_{34} – меры, реализуемые с целью дополнительных исследований на предмет наличие ST-канала.

Рис. 27. Декомпозиционное представление мероприятий по техническому контролю эффективности защиты информации от утечки по ST-каналу
Fig. 27. Decomposition view of activities for technical control of the effectiveness of data leakage protection via the ST channel

Третий уровень декомпозиции целевой функции «Противодействие утечке информации по ST-каналу» образуется путем детализации действий, выполняемых в процессе реализации мер E_{11}–E_{34}. Соответствующие данному уровню действия следует рассматривать как функции, реализующие указанные меры.

К функциям, реализующим меры по изменению конфигурации электронного оборудования СВТ (меры E_{11}), относятся (рис. 28):

K_{111} – функция замены аппаратных составляющих электронного оборудования СВТ случайным образом;

K_{112} – функция изменения аппаратной конфигурации электронного оборудования СВТ.

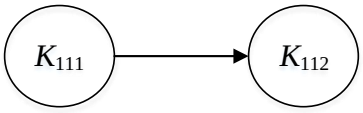


Рис. 28. Декомпозиционное представление мер по изменению конфигурации электронного оборудования СВТ

Fig. 28. Decomposition view of measures to change the configuration of electronic equipment of CT

К функциям, реализующим меры по замене импортного программно-аппаратного обеспечения СВТ на отечественное (меры E_{12}), относятся (рис. 29):

K_{121} – функция замены импортного программного обеспечения на отечественное;

K_{122} – функция замены импортного аппаратного обеспечения на отечественное.

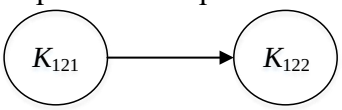


Рис. 29. Декомпозиционное представление мер по замене импортного программно-аппаратного обеспечения СВТ на отечественное

Fig. 29. Decomposition view of measures to replace imported hardware and software with domestic hardware of CT

К функциям, реализующим меры по проведению исследований на соответствие требованиям по безопасности информации (меры E_{21}), относятся (рис. 30):

K_{211} – функция проведения специальных проверок СВТ;

K_{212} – функция проведения специальных исследований СВТ.

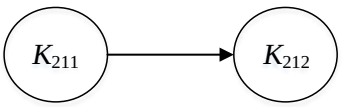


Рис. 30. Декомпозиционное представление мер по проведению исследований на соответствие требованиям по безопасности информации

Fig. 30. Decomposition view of measures to ensure compliance of the research activities with information security requirements

К функциям, реализующим меры по проведению дополнительных исследований (меры E_{22}), относятся (рис. 31):

K_{221} – функция формирования статистического профиля работы СВТ;

K_{222} – функция создания профиля помехи;

K_{223} – функция сравнения статистического профиля работы СВТ с эталонными образцами.

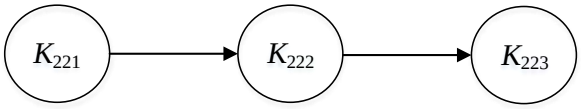


Рис. 31. Декомпозиционное представление мер по проведению дополнительных исследований
Fig. 31. Decomposition view of measures for additional research

К функциям, реализующим меры пассивной защиты информации (меры E_{31}), относятся (рис. 32):

K_{311} – функция полного или частичного экранирования помещения, в котором размещено СВТ;

K_{312} – функция полного или частичного экранирования СВТ.

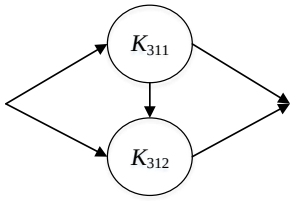


Рис. 32. Декомпозиционное представление мер пассивной защиты информации
Fig. 32. Decomposition view of passive information protection measures

К функциям, реализующим меры активной защиты информации (меры E_{32}), относятся (рис. 33):

K_{321} – функция применения генератора шума широкополосной помехи;

K_{322} – функция применения генератора шума прицельной помехи.

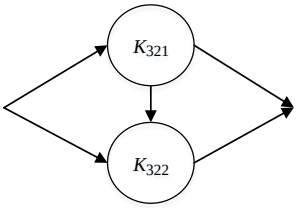


Рис. 33. Декомпозиционное представление мер активной защиты информации
Fig. 33. Decomposition view of active information protection measures

К функциям, реализующим меры, реализуемые с целью оценки эффективности защиты информации от утечки по ST-каналу в соответствии требованиями по безопасности информации (меры E_{33}), относятся (рис. 34):

K_{331} – функция проведения экспертно-документального контроля эффективности защиты информации от утечки по ST-каналу;

K_{332} – функция проведения инструментального контроля эффективности защиты информации от утечки по ST-каналу.

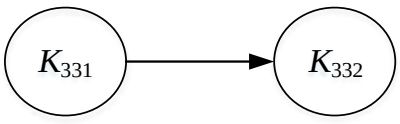


Рис. 34. Декомпозиционное представление мер, реализуемых с целью оценки эффективности защиты информации от утечки по ST-каналу в соответствии требованиями по безопасности информации
Fig. 34. Decomposition view of measures implemented to assess the effectiveness of the information leakage protection via the ST channel in accordance with information security requirements

К функциям, реализующим меры, реализуемые с целью дополнительных исследований на предмет наличие ST-канала (меры E_{34}), относятся (рис. 35):

K_{341} – функция анализа программного обеспечения СВТ на предмет обнаружения фрагментов кода, инициирующего модуляцию;

K_{342} – функция контроля времени работы электронного оборудования СВТ;

K_{343} – функция использования аппаратных верификаторов работы интерфейсов передачи данных электронного оборудования СВТ;

K_{344} – функция периодического контроля статистического профиля работы СВТ.

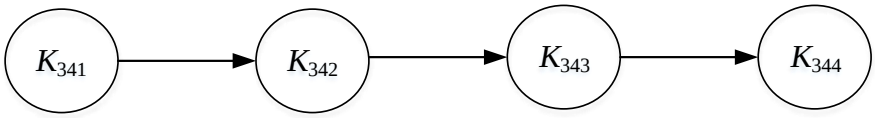


Рис. 35. Декомпозиционное представление мер, реализуемых с целью дополнительных исследований на предмет наличие ST-канала

Fig. 35. Decomposition view of measures implemented to allow additional research on the presence of an ST channel

Заключение

Традиционно в практике технической защиты информации для анализа защищенности объектов информатизации от утечки по техническим каналам разработаны соответствующие методики, основанные на экспертном анализе субъектно-объектных взаимосвязей между источниками угроз утечки информации и ее уязвимостями к такого рода угрозам. При этом данные методики не учитывают те случайные состояния исследуемых процессов, которые характеризуют их динамику.

Функциональное моделирование дает возможность представить случайные состояния процессов перехвата информативных сигналов СВТ по ST-каналу и противодействия утечке информации в терминах Марковских процессов. Подобное представление является предпосылкой для разработки математических моделей временных характеристик рассматриваемого типа угроз и мер реагирования на их проявление, что, в итоге, позволяет количественно оценить эффективность противодействия утечке информации по ST-каналу с учетом динамики его возникновения, продолжительности утечки и проводимых мероприятий по обеспечению защищенности информации. Естественно, что в этих условиях адекватность оценки защищенности информации будет выше адекватности оценки, полученной с помощью существующих методик.

СПИСОК ЛИТЕРАТУРЫ:

1. Хорев А.А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники. Специальная техника. 2010, № 2, с. 39–57. URL: https://www.elibrary.ru/item.asp?id=15134772 (дата обращения: 20.12.2021).
2. Кузнецов Ю.В., Баев А.Б., Коновалюк М.А., Горбунова А.А. Исследование непреднамеренных электромагнитных излучений средств вычислительной техники. Специальная техника. 2017, № 1, с. 2–15. URL: https://www.elibrary.ru/item.asp?id=29243415 (дата обращения: 20.12.2021).
3. Гончаров Н.И., Сирота А.А., Гончаров И.В. Анализ защищённости сетевых систем обработки данных по отношению к техническим каналам утечки информации. Специальная техника. 2017, № 1, с. 39–47. URL: https://www.elibrary.ru/item.asp?id=29243426 (дата обращения: 20.12.2021).
4. Авдеев В.Б., Анищенко А. В., Петигин А.Ф. Методический подход к оценке защищённости информации, обрабатываемой компьютером с использованием сложных сигналов, от утечки за счёт побочных электромагнитных излучений. Специальная техника. 2017, № 3, с. 40–47. URL: https://www.elibrary.ru/item.asp?id=29368071 (дата обращения: 20.12.2021).

5. Kuhn M.G. and Anderson R.J. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. In Information Hiding (1998), D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Springer, p. 124–142. DOI: https://doi.org/10.1007/3-540-49380-8_10.
6. Краева Е.В., Татарникова Т.М., Веревкин С.А., Миклуш В.А., Богданов П.Ю., Мартын И.А. Актуальность стеганографии и ее практическое применение. Информационные технологии и системы: управление, экономика, транспорт, право. СПб.: ООО «Андреевский издательский дом». 2019, № 3 (35), с. 105–109. URL: https://www.elibrary.ru/item.asp?id=41880024 (дата обращения: 20.12.2021).
7. Касперский Е.В. Компьютерное zловредство. СПб.: Издательство «Питер». 2007. – 208 с.
8. Markus G. Kuhn. Security Limits for Compromising Emanations (англ.). Cryptographic Hardware and Embedded Systems: журнал. 2005, vol. 3659, p. 265–279. DOI: http://dx.doi.org/10.1007/11545262_20.
9. Guri M.; Kedma G.; Kachlon A.; Elovici Y. (October 2014). AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE). P. 58–67. DOI: http://dx.doi.org/10.1109/MALWARE.2014.6999418.
10. Guri, M.; Monitz, M.; Elovici, Y. (December 2016). USBee: Air-gap covert-channel via electromagnetic emission from USB. 2016 14th Annual Conference on Privacy, Security and Trust (PST). P. 264–268. DOI: http://dx.doi.org/10.1109/PST.2016.7906972.
11. Guri M.; Monitz M.; Mirski Y.; Elovici Y. (July 2015). BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations. 2015 IEEE 28th Computer Security Foundations Symposium. P. 276–289. DOI: http://dx.doi.org/10.1109/CSF.2015.26.
12. Лиходедов Д.Ю., Волкова С.Н. О некоторых особенностях функционального представления деятельности по защите информации от утечки по техническим каналам. Охрана, безопасность и связь – 2011: материалы Международной научно-практ. конф. Часть 1. Воронеж: Воронежский институт МВД России. 2012, с. 195–198. URL: https://socionet.ru/publication.xml?h=spz:neicon:radioprom:y:2021:i:2:p:22-34&l=en (дата доступа:20.12.2021).
13. Волкова С.Н., Дерябин А.С. Функциональное моделирование, как инструмент исследования механизмов защиты информации. Информация и безопасность. Воронеж: ВГТУ. 2010, Вып. 2, с. 303–304. URL: https://www.elibrary.ru/item.asp?id=15122817 (дата доступа:28.02.2022)
14. Скрыль С.В., Крылов В.О., Филева С.А, Гуляев О.А. Функциональное представление угроз утечки информации по виброакустическим каналам на объектах авиакосмической промышленности. Авиакосмическое приборостроение. М: «Научтехлитиздат». 2017, № 12, с. 22–32. URL: https://www.elibrary.ru/item.asp?id=30740965 (дата доступа:28.02.2022)
15. Ревюз Д. Цепи Маркова / пер. с англ. М.: РФФИ, 1997. – 432 с.
16. Скрыль С.В., Сычев М.П. и др. Направления развития существующей концепции оценки актуальности угроз утечки информации по техническим каналам в условиях современных тенденций совершенствования технической разведки. Радиопромышленность. М: АО «ЦНИИ «Электроника». 2021, т. 31, № 1, с. 74–83. URL: https://www.elibrary.ru/item.asp?id=45540861 (дата обращения: 20.12.2021).

REFERENCES:

[1] Chorev A.A. Technical channels of information leakage processed by computer equipment. Specialnaya Technika. 2010, no.2, p. 39–57. URL: https://www.elibrary.ru/item.asp?id=15134772 (accessed: 20.12.2021) (in Russian).
[2] Kuznetsov Y.V., Bayev A.B., Konovaluk M.A., Gorbunova A.A. Research on unintentional electromagnetic emissions of computer equipment. Specialnaya Technika [Special Technique]. 2017, no. 1, p. 2–15. URL: https://www.elibrary.ru/item.asp?id=29243415 (accessed: 20.12.2021) (in Russian).
[3] Goncharov N.I., Sirota A.A., Goncharov I.V. Analysis of the security of data processing network systems in connection with technical channels of information leakage. Specialnaya Technika [Special Technique]. 2017, no.1, p. 39–47. URL: https://www.elibrary.ru/item.asp?id=29243426 (accessed: 20.12.2021) (in Russian).
[4] Avdeeva V.B., Anischenko A.V., Petigin A.F. A methodological approach to assessing the security of computer-processed information using complex signals from leakage due to transient electromagnetic pulse emanation. Specialnaya Technika [Special Technique]. 2017, no. 3, p. 40–47. URL: https://www.elibrary.ru/item.asp?id=29368071 (accessed: 20.12.2021) (in Russian).
[5] Kuhn M.G. and Anderson, R.J. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. In Information Hiding (1998), D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Springer, p. 124–142. DOI: https://doi.org/10.1007/3-540-49380-8_10.

[6] Krayeva E.V., Tatarnikova T.M., Verevkin S.A., Mikluch V.A., Bogdanov P.Y., Martyn I.A. The relevance of steganography and its practical application. Informatsionnie technologii I sistemi: upravlenie, economika, transport, pravo [Information technology and systems: management, economics, transport, law.], Saint-Petersburg, Andreevskii izdatelskiy dom Publ. 2019, no. 3 (35), p. 105–109. URL: https://www.elibrary.ru/item.asp?id=41880024 (accessed: 20.12.2021) (in Russian).

[7] Kaspersky E.V. Komputernoe zlovredstvo [Computer malware.], Saint-Petersburg, Piter Publ. 2007. – 208 p. (in Russian).

[8] Markus G. Kuhn. Security Limits for Compromising Emanations. Cryptographic Hardware and Embedded Systems: журнал. 2005, vol. 3659, p. 265–279. DOI: http://dx.doi.org/10.1007/11545262_20.

[9] Guri M.; Kedma G.; Kachlon A.; Elovici Y. (October 2014). AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE). P. 58–67. DOI: http://dx.doi.org/10.1109/MALWARE.2014.6999418.

[10] Guri, M.; Monitz, M.; Elovici, Y. (December 2016). USBee: Air-gap covert-channel via electromagnetic emission from USB. 2016 14th Annual Conference on Privacy, Security and Trust (PST). P. 264–268. DOI: http://dx.doi.org/10.1109/PST.2016.7906972.

[11] Guri M.; Monitz M.; Mirski Y.; Elovici Y. (July 2015). BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations. 2015 IEEE 28th Computer Security Foundations Symposium. P. 276–289. DOI: http://dx.doi.org/10.1109/CSF.2015.26.

[12] Likhodedov D.Yu., Volkova S.N. On some features of the functional representation of activities to protect information from leakage through technical channels. Protection, security and communication – 2011: materials of the international scientific and practical. conf. Part 1. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia. 2012, p. 195–198. URL: https://socionet.ru/publication.xml?h=spz:neicon:radioprom:y:2021:i:2:p:22-34&l=en (accessed:20.12.2021) (in Russian).

[13] Volkova S.N., Deryabin A.S. Functional modeling as a tool for studying the mechanisms of information protection. Information and security. Voronezh: VSTU. 2010, Issue. 2, p. 303–304. URL: https://www.elibrary.ru/item.asp?id=30740965 (accessed:28.02.2022) (in Russian).

[14] Skryl S.V., Krylov V.O., Fileva S.A., Gulyaev O.A. Functional representation of threats of information leakage through vibroacoustic channels at objects of the aerospace industry. Aerospace instrumentation. Moscow: «Nauchtekhlitizdat». 2017, no. 12, p. 22–32. URL: https://www.elibrary.ru/item.asp?id=15122817 (accessed:28.02.2022) (in Russian).

[15] Revuz D. Markov Chains. per. from English - M.: RFBR, 1997. – 432 p. (in Russian).

[16] Skryl S.V., Sychev M.P. et al. Directions for the development of the existing concept of assessing the relevance of information leakage threats through technical channels in the context of modern trends in improving technical intelligence. Radio industry. M: JSC "Central Research Institute" Electronics ". 2021, v. 31, no. 1, p. 74–83. URL: https://www.elibrary.ru/item.asp?id=45540861 (accessed: 20.12.2021) (in Russian).

Поступила в редакцию – 27 декабря 2021 г. Окончательный вариант – 05 февраля 2022 г.
Received – December 27, 2021. The final version – February 05, 2022.

Рукописи, предоставляемые в редакцию, должны соответствовать следующим требованиям:

– тема статьи должна быть актуальной, иметь научное или практическое значение и публиковаться авторами впервые;

– рукопись должна быть оформлена только в формате *.doc или *.docx, полоса А4, кегль 12, шрифт TimesNewRoman, интервал одинарный;

– в начале статьи идут сведения о статье **на русском языке**: Имя О. Фамилия авторов (по центру, строчными буквами, кегель 12); далее сведения об авторах – организация с почтовым адресом, адрес электронной почты и личный идентификатор ORCID (по центру, строчными буквами, курсив, кегель 11); затем название статьи (по центру, ПРОПИСНЫМИ буквами, кегель 12), в случае выполнения статьи в рамках НИР, гранда и пр. возможно оформление сноски на благодарность; благодарность (курсивом, кегель 11) - пишутся сведения об источнике финансирования; ключевые слова (не более шести, по ширине, курсив, кегель 11); аннотация (100 – 250 слов, по ширине, строчными буквами – см. **правила оформления аннотации**);

– далее повторяются все сведения о статье **на английском языке.**

– название статьи на английском оформляется по центру, строчными буквами, полужирно с подчеркиванием;

– в статью включают **Введение** и **Заключение**, а также вводятся **Разделы** с их нумерацией (прописные по центру, полужирно, кегль 12);

– затем идет текст статьи на русском или английском языке, кегль 12, интервал одинарный, рекомендуемый общий объем статьи не должен превышать 10 страниц, включая таблицы, иллюстрации; подписи под иллюстрациями на русском языке дублируются на английском языке;

– в конце статьи приводится СПИСОК ЛИТЕРАТУРЫ, в котором указан библиографический список источников литературы литературы (по ширине, строчные, кегль 10), оформленный в соответствии с действующими стандартами и указанием идентификатора DOI (как правило, не менее 15 наименований в научной статье и 50 в обзорной статье);

– после списка литературы идет REFERENCES, в котором указанные библиографические данные авторов и название статьи должны быть на английском языке, исходные данные русскоязычного издания и издательства должны быть представлены в транслитерации на латиницу.

Правила оформления аннотации

Аннотация является источником информации о содержании статьи и изложенных в ней результатах исследований и дает возможность установить основное содержание статьи, определить его релевантность и решить, следует ли обращаться к полному тексту статьи. Аннотация используется в информационных, в том числе автоматизированных, системах для поиска документов и информации (на английский язык переводятся: название, аннотация и ключевые слова, и по ним зарубежный читатель судит о содержании статьи).

Структура аннотации должна соответствовать структуре статьи и должна быть объемом не менее 100 слов, но не более 250 слов.

Аннотация включает следующие аспекты содержания статьи**:**

- предмет, цель статьи;
- метод или методологию проведения научной работы, описываемой в статье;
- результаты научной работы;
- область применения результатов;
- выводы.

Аннотация к статье должна быть информативной (не содержать общих слов) и оригинальной. Сведения, содержащиеся в заглавии статьи, не должны повторяться в тексте аннотации. Текст аннотации не должен содержать интерпретацию содержания статьи, критические замечания и точку зрения автора, а также информацию, которой нет в статье. Следует избегать лишних вводных фраз (например, «автор статьи рассматривает...»).

Исторические справки, если они не составляют основное содержание статьи, описание ранее опубликованных работ и общеизвестные положения в аннотации не приводятся.

В тексте аннотации следует употреблять синтаксические конструкции, свойственные языку научных и технических документов, избегать сложных грамматических конструкций.

В тексте аннотации следует применять значимые (ключевые) слова из текста статьи.

Метод или методологию проведения работы целесообразно описывать в том случае, если они отличаются новизной или представляют интерес с точки зрения данной работы. В аннотации статьи, описывающей экспериментальные работы, указывают источники данных и характер их обработки.

Результаты работы описывают предельно точно и информативно. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи

и закономерности. При этом отдается предпочтение новым результатам и данным долгосрочного значения, важным открытиям, выводам, которые опровергают существующие теории, а также данным, которые, по мнению автора, имеют практическое значение.

Выводы могут сопровождаться рекомендациями, оценками, предложениями, гипотезами, описанными в статье.

Правила оформления текстов для публикации

1. Статьи необходимо подавать в электронном виде (файл *.doc) с распечаткой (или файлом в формате *.pdf) – во избежание неточностей прочтения формул.
2. Рисунки, графики, фотографии и другие виды иллюстраций следует предоставлять не только включенными в текст, но и отдельными файлами в исходном формате (не интегрированными в документ Word). Подписи под иллюстрациями делать на русском и английском языках.
3. Сокращения и аббревиатуры, которых нет в списке сокращений, необходимо раскрывать (в скобках или в сноске).
4. Давая в тексте статьи ссылки на формулы, выражения или ограничения, пожалуйста, убедитесь в том, что соответствующие объекты в статье есть и пронумерованы.
5. Ссылки на литературу следует давать в тексте в квадратных скобках, в случае цитирования – с указанием страниц.
6. При оформлении списка литературы обязательно проверить наличие и корректность выходных данных работ и исключить повторные указания одной и той же работы под разными номерами.
7. В список литературы не рекомендуется помещать источники старше 5 лет (рекомендация ВАК), а также источники, которых нет научных электронных базах (российские - это Elibrary, Ciberleninka).
8. Не надо помещать в список литературы анонимные источники - законы, нормативные акты, инструкции и пр. Их, при необходимости, помещать в постраничной ссылке или прямо по тексту.
9. Нельзя ссылаться на справочно-поисковые системы типа «Консультант» вместо ссылок на оригиналы.
10. Недопустимо в научной статье ссылаться на учебники и учебные пособия (на учебники допустимо ссылаться только в обзорных статьях).
11. Иноязычные слова, термины и фамилии, написание которых допускает варианты, просьба писать в пределах одной статьи одинаково.

Условия опубликования статьи:

– статья должна быть выслана по электронной почте, загружена самостоятельно на сайте журнала или представлена в редакцию на электронном носителе;

– редакционная коллегия журнала следует этическим нормам, принятым в международном научном сообществе, опираясь на рекомендации Комитета по этике научных публикаций, не противоречащим нормам российского законодательства в областях регулирования деятельности средств массовой информации и авторского права;

– статьи, не соответствующие установленным требованиям представления и оформления, не рассматриваются и не публикуются;

– в одном номере журнала публикуется, как правило, только одна статья автора, в том числе с соавторами;

– авторы должны предоставлять только оригинальные работы, при использовании текстовой или графической информации, полученной из работ других лиц, необходимы ссылки на соответствующие публикации или письменное разрешение автора;

– решение о публикации рукописи принимается редакционной коллегией на основании результата двойного слепого рецензирования и экспертной оценки квалифицированными специалистами в области ИБ, срок рецензирования не превышает 30 дней;

– в случае приема рукописи к публикации автор должен оперативно давать ответы на вопросы редакции, связанные с замечаниями по статье;

– в случае отказа в публикации редакционная коллегия должна предоставить автору копию рецензии и обоснование отказа в публикации;

– подача статьи в более чем в один журнал одновременно расценивается как неэтичное поведение и является неприемлемой;

– статьи публикуются бесплатно.

Заранее спасибо,
редакционная коллегия

СПИСОК СОКРАЩЕНИЙ, ПРИНЯТЫХ В ЖУРНАЛЕ

АБИ – администратор безопасности информации
АнД – аналоговый документ
АРМ АБИ – автоматизированное рабочее место администратора безопасности информации
АС – автоматизированная система
БД – база данных
БИС – большая интегральная схема
БЧ – блокчейн
ИБ – информационная безопасность
ИКТ – информационно-коммуникационные технологии
ИП – информационные продукты
ИПС – изолированная программная среда
ИР – информационные ресурсы
КПО – комплекс программного обеспечения
КСЗ – комплекс средств защиты
КТЭ – компьютерно-техническая экспертиза
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НД – нормативный документ
НСД – несанкционированный доступ
ОИ – объект информатизации
ОКСО – Общероссийский классификатор специальностей по образованию
ОС – операционная система
ПАК – программно-аппаратный комплекс
ПО – программное обеспечение
ПРД – правила разграничения доступа
ПСКЗИ – персональное средство криптографической защиты информации
РД – руководящий документ
РКБ – резидентный компонент безопасности
РПВ – разрушающее программное воздействие
СБЧ – система блокчейн
СВТ – средство вычислительной техники
СЗИ – средство защиты информации
СЗИ НСД – средство защиты информации от несанкционированного доступа
СКЗИ – система криптографической защиты информации
СРД – система разграничения доступа
СУБД – система управления базами данных
ЭлД – электронный документ
ЭЦП – электронная цифровая подпись
ФГОС – федеральный государственный образовательный стандарт
ФУМО ИБ – федеральное учебно-методическое объединение по образованию в области информационной безопасности

Адрес редакции: Каширское ш., 31, Москва, 115409, Россия
Тел.: +7 (495) 788 5699, тоновый режим 9216 или 8277

Editorial address: Kashirskoe shosse, 31, Moscow, 115409, Russia
Tel. +7 (495) 788 5699, tone mode set 9216 or 8277
E-mail: BIT@mephi.ru
Сайт журнала: https://bit.mephi.ru

Периодичность выхода – 4 раза в год / Periodicity – 4 times a year

Подписка на журнал
производится в почтовых отделениях связи
по каталогу «Пресса России»

Подписной индекс 29226

Цена в продаже свободная / Price selling free

Ответственный редактор И.М. Ядыкин
Технический редактор П.А. Золотухина

Подписано в печать 09.03.2022. Формат 60x84 1/8
Печ. л. 18,5 Уч.-изд. л. 18,5 Тираж 500 экз. Изд. № 002 – 3

Акционерное общество «Экспериментальное научно-производственное объединение
СПЕЦИАЛИЗИРОВАННЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ»
(АО «ЭНПО СПЭЛС»)
Каширское ш., 31, строение 44, этаж 3, пом. IV, ком. 4, Москва, 115409, Россия

Joint Stock Company «Experimental Scientific and Production Association
SPECIALIZED ELECTRONIC SYSTEMS»
(JSC «ENPO SPELS»)
Kashirskoe shosse, 31, building 44, floor 3, pom. IV, room 4, Moscow, 115409, Russia

Типография ООО «ТИПОГРАФИЯ»
ул. Кантемировская, 60, Москва, 115477, Россия